NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

COST-EFFECTIVENESS ANALYSIS OF
SYSTEM SAFETY

by

Alberta Rose Josephine Jones

March 1987

Thesis Advisor: Paul M. Carrick

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

1a REPORT SECURITY CLASSIFICATION UNCLASSIFIED	1b RESTRICTIVE MARKINGS
2a SECURITY CLASSIFICATION AUTHORITY	3 DISTRIBUTION / AVAILABILITY OF REPORT Approved for public release; distribution is unlimited
2b DECLASSIFICATION / DOWNGRADING SCHEDULE	
4 PERFORMING ORGANIZATION REPORT NUMBER(S)	5 MONITORING ORGANIZATION REPORT NUMBER(S)
6a NAME OF PERFORMING ORGANIZATION Naval Postgraduate School 6b OFFICE SYMBOL (If applicable) Code 54	7a NAME OF MONITORING ORGANIZATION Naval Postgraduate School
6c ADDRESS (City, State, and ZIP Code) Monterey, California 93943-5000	7b ADDRESS (City, State, and ZIP Code) Monterey, California 93943-5000
8a NAME OF FUNDING / SPONSORING ORGANIZATION 8b OFFICE SYMBOL (If applicable)	9 PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
8c ADDRESS (City, State, and ZIP Code)	10 SOURCE OF FUNDING NUMBERS PROGRAM ELEMENT NO. / PROJECT NO. / TASK NO. / WORK UNIT ACCESSION NO

11 TITLE (Include Security Classification)
COST-EFFECTIVENESS ANALYSIS OF SYSTEM SAFETY

12 PERSONAL AUTHOR(S)
Jones, Alberta R.

13a TYPE OF REPORT	13b TIME COVERED	14 DATE OF REPORT (Year, Month, Day)	15 PAGE COUNT
Master's Thesis	FROM _____ TO _____	1987, March	146

16 SUPPLEMENTARY NOTATION

17 COSATI CODES			18 SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
FIELD	GROUP	SUB-GROUP	System Safety; Cost-Effectiveness; Cost-Benefit Analysis

19 ABSTRACT (Continue on reverse if necessary and identify by block number)

The Department of Defense (DOD) Instruction 5000.36, "System Safety Engineering and Management," directs the Department of the Navy to establish formalized system safety programs throughout the procurement and life cycle of all systems, subsystems and equipment, and modifications thereto, acquired by DOD. Ideally, the application of system safety engineering and management techniques improves the mission net cost-effectiveness of any DOD weapon system by the prevention of accidental deaths and injuries, and by minimizing material losses and damage to operational systems. Even though DOD has directed significant attention to the incorporation of system safety in current and future weapon systems, the system safety program has been criticized for its poor marginal contribution. In the past, Naval system safety programs have struggled for survival and recognition. With this in mind, the scope of this thesis is to evaluate the cost-effectiveness of system safety.

20 DISTRIBUTION / AVAILABILITY OF ABSTRACT	21 ABSTRACT SECURITY CLASSIFICATION
☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT. ☐ DTIC USERS	Unclassified
22a NAME OF RESPONSIBLE INDIVIDUAL Prof. Paul M. Carrick PMCarrick	22b TELEPHONE (Include Area Code) (408) 646-2939 22c OFFICE SYMBOL Code 54Ca

DD FORM 1473, 84 MAR 83 APR edition may be used until exhausted. All other editions are obsolete.

SECURITY CLASSIFICATION OF THIS PAGE
UNCLASSIFIED

Approved for public release; distribution is unlimited

Cost-Effectiveness Analysis of System Safety

by

Alberta Rose Josephine Jones
Lieutenant, United States Navy
B.S., Oklahoma State University, 1978

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
March 1987

ABSTRACT

The Department of Defense (DOD) Instruction 5000.36, "System Safety Engineering and Management," directs the Department of the Navy to establish formalized system safety programs throughout the procurement and life cycle of all systems, subsystems and equipment, and modifications thereto, acquired by DOD. Ideally, the application of system safety engineering and management techniques improves the mission net cost-effectiveness of any DOD weapon system by the prevention of accidental deaths and injuries, and by minimizing material losses and damage to operational systems. Even though DOD has directed significant attention to the incorporation of system safety in current and future weapon systems, the system safety program has been criticized for its poor marginal contribution. In the past, Naval system safety programs have struggled for survival and recognition. With this in mind, the scope of this thesis is to evaluate the cost-effectiveness of system safety.

TABLE OF CONTENTS

ACKNOWLEDGMENTS

I express sincere appreciation to Dr. Donald M. Layton who provided invaluable assistance in helping me to understand the system safety concept and to my thesis advisor, Dr. Paul Carrick, and second reader, LCDR Dale Scoggin, for their suggestions and assistance. I would also like to thank the following people and field activities: Messrs. Jim Gibble, Jim Nerrie, Jack Copeland, Dave Marcinick, Richard Olson, Paul Kinzey, LT Barry Graham (USAF), Dr. S.P. Dunlap, and the fine staff at the Naval Aviation Safety School, Monterey, California, and the System Safety Engineering Department, Naval Air Engineering Center, Lakehurst, New Jersey.

I. INTRODUCTION

A. NATURE OF THE PROBLEM

The Department of Defense (DOD) and the Department of the Navy (DON) have directed attention toward maintaining operational readiness through early recognition of hazards (see Figure 1.1) to prevent the loss or degradation of systems. DODINST 5000.36 and OPNAVINST 5100.24A provide policy requirements for DOD and DON system safety programs. Program requirements are detailed in MIL-STD882B, "System Safety Program Requirements."

The Navy System Safety policy states that system Safety Management Controls shall be applied to all Acquisition Category[1] I and II programs throughout the system's or facility life cycle. Program sponsors, acquisition commands and their field activities shall selectively apply these controls to all acquisitions and military construction projects, system maintenance programs, logistics training and operations and research programs leading to new systems acquisitions. Engineering and management controls shall be

---

[1]Acquisition Category (ACAT)--DON programs are classified by ACATs which determine their level of review. Programs are assigned an ACAT, i.e., I, II, III, or IV; when first authorized based on estimated cost, criticality, and political sensitivity. ACAT I-thresholds are $200 million (Fiscal Year (FY) 80 dollars) in RDT&E funds or $1 billion (FY 80 dollars) in procurement funds or both. ACAT II-total costs are expected to exceed $100 million for RDT&E and/or $500 million for procurement (FY 80 dollars).

Hazard. An existing or potential condition that can result in creating any of the four levels shown in this example. A hazard is considered a prerequisite to a mishap.

MIL-STD-882B		EFFECT ON	
Level	Mission Fulfillment	Functional Capabilities	Personnel Safety
I Catastrophic	Lost	Aircraft Total Loss Weapon Premature Firing High Voltage	Death or Severe Injury Loss of Job
II Critical	Lost	Aircraft Major Damage (over 500 MMHRS to repair) Weapon: Loss/non-Repairable Damage	Major injury (One or more days lost)
III Marginal	Impaired (But capable of completion)	Aircraft minor damage (over 100 MMHRS to repair weapon: requires intermediate or depot level repair Ground support equipment Loss or non-repairable damage	Minor Injury (one day or less)
IV Negligible	Unimpaired	Aircraft: Non (zero to 100 MMHRS) to repair) weapon: requires organizational level repair. Ground support equipment: repairable damage	First aid (no lost time)

Figure 1.1 System Safety Hazard Severity for a Weapon (Example)

applied through suitable tailoring of MIL-STD-882B to ensure that primary emphasis is placed on the identification, evaluation, and elimination/control of hazards prior to system production/construction and deployment.

A study by the Logistics Management Institute made the following comments regarding system safety in aircraft acquisition:

> The cost of Military aviation mishaps and safety modification and retrofit programs exceeds $1 billion and entails the loss of over 200 lives and 200 aircraft annually. Better implementation of the Department of Defense's system safety policies, plus some refinements in those policies, can reduce these losses.
>
> Successful system safety programs hold valuable lessons for DoD.
>
> - System safety investments can and do pay off. National Aeronautics and Space Administration's (NASA's) Manned Space Flight Program has had an intensive effort, with heavy involvement of top management, in system safety since the early Apollo fire. Their policy is, simply, "no accidents."[2] It works.
>
> - System safety does not require large investments to be cost-effective. For example, a typical system safety program investment (about $5 to $10 million over 10 years for a major program) is well worthwhile if it only results in preventing the loss of a single aircraft ($15 million for the AH-64, $25 million for the F-18, $200 million for the B-1B).
>
> - An effective system safety program requires top management interest and support. In the acquisition process, the immediacies are schedule, performance, and especially cost. Benefits from investments in system safety show up primarily in the long run and

---

[2]This statement was factual until January 28, 1986, when the loss of the space shuttle Challenger and all its crew occurred in part because of an ineffective "silent safety program" within NASA that allowed critical solid rocket booster deficiencies to be treated as acceptable flight risks. [Ref. 1:p. 19]

> then are observable only indirectly (i.e., as non-accidents and the avoidance of safety modifications). Investments in system safety are easily deferred by those directly involved in an acquisition program. Therefore, it is essential to have interest and support of system safety by "offline" management at levels high enough to be effective. [Ref. 2:pp. v-vi]

In the later part of 1986, the Naval Safety Center requested funds for system safety for the following reasons:

> System Safety Engineering is not being properly incorporated into naval acquisitions. Specific problem areas, highlighted by the Navy Inspector General, include starting system safety programs too late, failure to include system safety engineering as a life cycle process, use of untrained Navy personnel as principals for safety, use of unqualified personnel at contractor's facilities to perform system safety analysis, and failure of program managers to include any system safety requirements to a large number of acquisitions. A significant problem identified during Logistics Review Group audits is the failure to track and correct known hazards. As a result, the Navy establishment is suffering unneeded personnel loses, injuries, system losses, and damage. These safety mishaps combine to degrade operational readiness and increase overall operating costs because engineering changes are necessary to correct safety deficiencies. Cost savings for an effective system safety program are estimated as a minimum, at 4 to 1 over investment,and are usually recouped by preventing the need for costly engineering changes estimated at $1 million each or more. [Ref. 3:p. 1]

The Naval Safety Center statement appears to be a declaration of the failure by DON to properly ensure that system safety requirements are achieved during the development of a weapon system or facility as required by DODINST 5000.36 and OPNAVINST 5100.24A. This research concentrates on the responsibilities required of DON to accomplish an effective system safety effort and what cost-benefits will be achieved from doing so.

B. AREA OF RESEARCH

Research will be conducted to determine the cost effectiveness of having a system safety program within the Department of the Navy (DON).

C. RESEARCH QUESTIONS

The primary research question is:

1. Is it cost effective to have a system safety program?
2. The subsidiary research questions are:

    a. How do we determine the effectiveness of system safety?

    Can the effectiveness of system safety be measured?

    b. Are current system safety programs within the Navy being managed more or less efficiently? (i.e., are there enough resources to do the job effectively or are there too many resources being extended.)

    c. What does it cost to make safety changes/modifications to a weapon system after fleet introduction? Could these changes have been made earlier?

    d. How are safety lessons learned (documented safety hazards from previous weapon systems) subsequently incorporated into the design process? Does maintaining historical system safety data (lessons learned) decrease the future costs of maintaining an effective system safety program?

D. METHODOLOGY

In order to answer the primary and subsidiary research questions, a combination of research techniques were used: (1) A literature search was conducted to gather, analyze, and summarize data on system safety and cost-beenfit/cost-effectiveness techniques; (2) Personal interviews with key professionals within NAVAIRSYSCOM, tenant activities and

supporting agencies were conducted. The data obtained through the literature search and personal interviews was used to postulate an appropriate measure of how to value the cost-effectiveness of system safety.

E. ORGANIZATION OF THESIS

Chapter I states the reason for the basic problem area being studied, identifies the primary and subsidiary research questions and the intended methodology to be used to answer the research questions.

Chapter II provides an in-depth review of what the concept being studied is and the history of the concept. The issue of system safety program support in the development of aircraft weapon systems is addressed in detail. The chapter concludes with the need for more resources being devoted to the system safety concept.

Chapter III contains reviews of the following system safety topics:

1) system safety program requirements and how important the role of the organizational element within DOD assigned acquisition management responsibility for system safety is;

2) system safety objectives and the need for providing a balance between management controls and system safety risks; and

3) the system safety process is reviewed in order to provide a logical approach to obtaining system safety objectives.

Chapter IV defines benefit-cost and cost-effectiveness analysis (BCA/CEA). The history of BCA is provided along

with specific requirements of Executive Order 12291 (the most recent regulatory requirements pertaining to BCA). The chapter concludes with a discussion of the difficulty involved in doing a BCA on safety-related issues.

Chapter V discusses the term System Engineering and System Engineering Specialties. System Safety is identified as a system engineering specialty and is considered a prerequisite to attaining cost, schedule, and technical performance objectives in the development of a weapon system. A 10 step standardized approach to conducting a system engineering cost-effectiveness evaluation is provided. Each step is briefly described. The chapter concludes by defining what "system effectiveness" is. A multi-attribute system effectiveness model is reviewed. System Safety isn't currently considered a major program objective in the multi-attribute model but could be if it was identified as such. In conclusion, system effectiveness models could be considered as one possible way of determining the cost-effectiveness of system safety.

Chapter VI contains a summary of the analysis and provides conclusions.

F. BENEFITS OF THE THESIS

The Joint Services System Safety Panel and NAVAIRSYSCOM's System Safety Department (09F) have requested assistance in analyzing the cost effectiveness of system safety.

This study will contribute to finding an appropriate measure.

II. BACKGROUND AND DISCUSSION

The first section of this chapter contains a description of what system safety is. This section is intended to provide an understanding of the system safety concept and the difficulty involved in measuring its cost and benefits in the development of a weapon system.

The second section contains a review of the history of system safety. This section provides necessary background information concerning the current level of system safety effort within DON.

The chapter concludes by addressing the need to establish high level positions within DOD devoted to system safety, and more specifically a need for more resources being devoted to system safety at the Naval Air Systems Command level.

A. WHAT IS SYSTEM SAFETY?

In 1972 the Army Safety Center in a technical report made the following statement regarding system safety:

> System safety as a discipline has not existed long enough for the definitions of terms it uses to become universally understood and accepted. A common problem in understanding and evaluating a System Safety Program stems from various definitions of the same terms being used which leads to confusion and misunderstanding. [Ref. 4:p. 1]

A much more recent Air Force document stated:

> It is difficult to explain the "why" and "hows" of the System Safety discipline when there is a lack of agreement

within the discipline as to just what the task really is. At a meeting of approximately 50 system safety engineers, each engineer was asked to provide a definition of system safety. Of these 50 fully-qualified and experienced System Safety engineers, at least 30 had distinctly different ideas of what constitutes the system safety task. Very little standardization currently exist between agencies or even between the directives, regulations, and standards that implement the requirement. [Ref. 5:p. 1-2]

The Department of the Air Force's Space Division Headquarters puts the function of system safety into the framework of a mishap[1] risk[2] management program. For their purposes, System Safety is discussed as: "A system engineering approach to risk management which involves the detection of systems, subsystems, components, or test and operational sequences which have an element of risk." [Ref. 5:p. 1-2] In this context, the system safety program is oriented in terms of program management as well as design or development task performance. It examines the interrelationships of all components of a program and its systems with the objective of bringing mishap risk or risk reduction into the management review process for automatic consideration in total program perspective. It involves the preparation and implementation of system safety program

---

[1]Mishap--an unplanned event or series of events that result in death, injury, occupational illness or damage to or loss of equipment or property.

[2]Risk--an expression of the possibility of a mishap in terms of hazard severity and hazard probability. Risk design goals are illustrated in Figure 2.1.

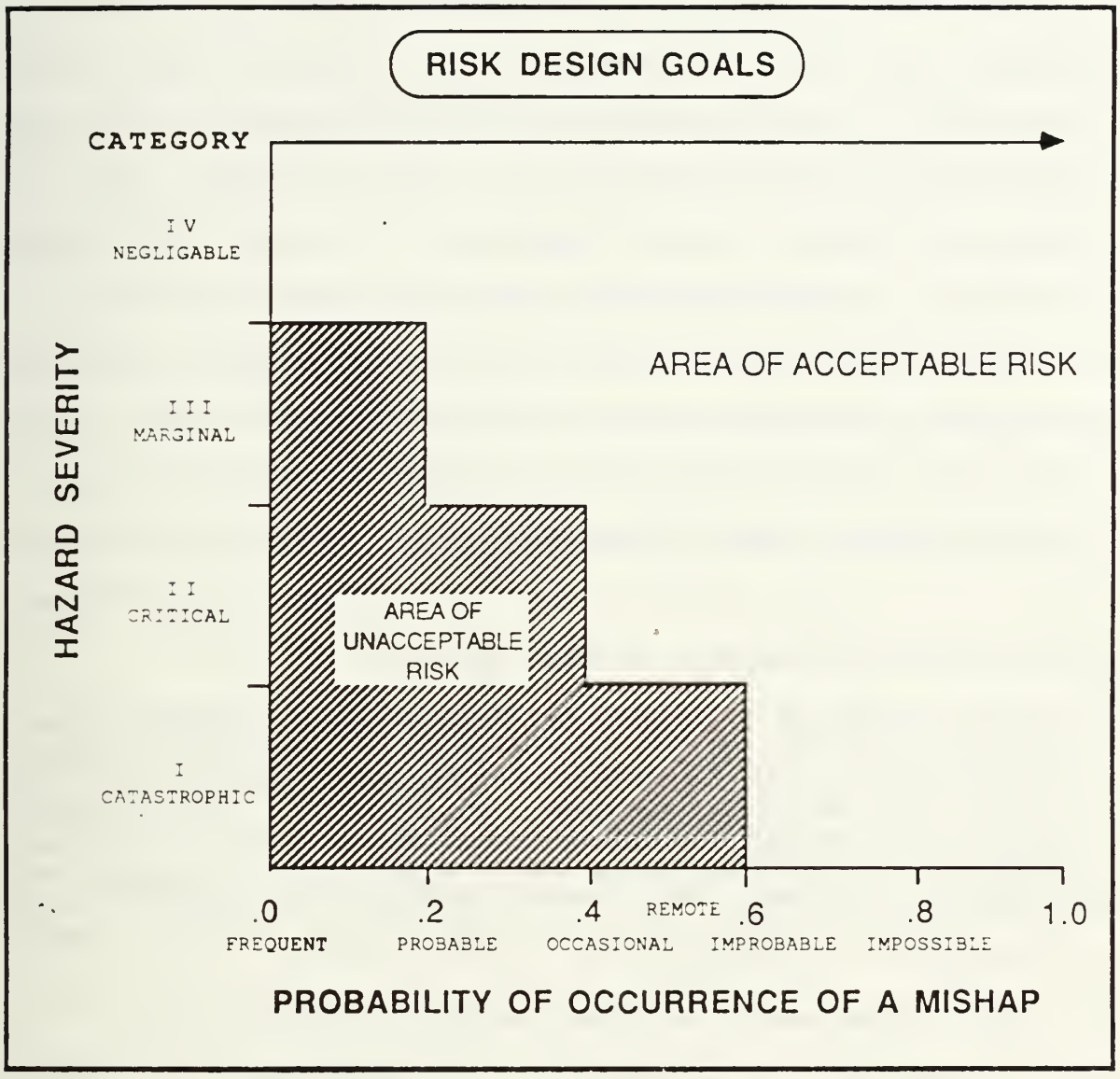


Figure 2.1 Risk Design Goals

plans[3]; also, the performance of system safety analyses on both system design and operations, and risk assessment in support of both management and system engineering activities. The system safety activity provides the program manager with a means of identifying what the mishap risk is, where a mishap can be expected to occur, and what alternative routes the design can make. [Ref. 5:p. 1-2]

Even though there seems to be no universally accepted definition of system safety, the two most widely used references pertaining to system safety define it as follows.

The System Safety Engineering and Management manual which is intended to be the practicing system safety professional's reference manual states:

> System safety is the application of special technical and managerial skills to the systematic, forward-looking identification and control of hazards through the life cycle of a project, program, or activity. The concept calls for safety analyses and hazard control actions, beginning with the conceptual phase of a system and continuing through the design, production, testing, use and disposal phases, until the activity is retired. [Ref. 6:p. 9]

Military Standard 882B defines system safety as:

> The application of engineering and management principles, criteria, and techniques to optimize safety within the constraints of operational effectiveness, time, and cost throughout all phases of the system life cycle. [Ref. 7:p. 3]

---

[3]System safety program plan--a description of the planned methods to be used by the contractor to implement the tailored requirements of MIL-STD-882B, including organizational responsibilities, resources, methods of accomplishment, milestones, depth of effort, and integration with other program engineering and management activities and related systems.

Note the thrust and emphasis of this definition ". . . within the constraints of operational effectiveness, time and cost. . . ." This is not safety at any cost, but safety within the constraints of the real world. [Ref. 8:p. 101] Thus, system safety is a principal contributor to the understanding and management of risk, with the objective of reducing the cost of mishaps and the need for costly safety-driven modifications after the system is put into operational use. This reflects where we are in the real world today. The current attitude towards system safety is that one should find the best and safest way to perform desired mission functions.

A formalized system safety program therefore provides the program manager with an effective means of identifying what risk elements exist and a means to evaluating their interrelationship to all elements of a program. These risk elements are most significant in the preventive mode and are detected by system safety hazard analysis techniques (i.e., determine where a mishap can be expected to occur and provide an alternative design approach), and when corrected by a design action results in either the control of, the elimination of, or the softening of those effects identified in the resultant mishap.

System safety is also a discipline which addresses all aspects of safety, having its greatest impact when applied during the early design and development stages of a new

system. Its basic orientation is to the total "system," and includes anything that could cause or prevent accidents (e.g., hardware, software, people, environment). Particular care must be is given to subsystem interfaces, since that is where accidents most often originate. [Ref. 2:p. 1-1]

A way of illustrating what system safety is to examine case histories. Success (or failure) stories aren't logged formally. However, examples abound where system safety personnel identified hazards which were corrected before accidents occurred and well before the problem would have been identified otherwise. [Ref. 2:p. 1-4] The following examples are illustrative:

- During the design of the F-18, an increase in fire hazard was avoided when a system safety engineer convinced program decision makers that a proposed increase in allowable bleed air duct temperature was dangerous. It was also pointed out that a similar hazard could be avoided by ensuring that the bleed air shutoff valve closed when power was removed. A change was made accordingly.

- During a modification to the B-52, a system safety engineer noted that if the front lugs of the air launched Cruise Missile attachment retracted but the rear ones did not, parts of the pylon would tear from the wing and, together with the missile, would inflict severe structural damage to the wing and possibly the horizontal stabilizer. The system was redesigned.

- In a similar case, the CH-47D originally had a single-point hook for load lifting. To improve load retention, a three-point attachment was designed. The system safety engineer discovered that if one hook were to hang up with the others open, it was quite probable that the aircraft could not be controlled, and a good chance existed that cables might actually contact rotor blades. The redesign assured that all hooks opened or none of them did.

- A safety engineer found in the PAVE LOW helicopter system that loss of voltage in a radar circuit would cause a command to the aircraft to fly at zero altitude with no warning to the pilot. He also checked with personnel on the RF-4C and A7D programs, knowing they used the same system. All aircraft were quickly prohibited from flying certain low-level missions until the systems were corrected. [Ref. 2:p. 1-5]

The NASA/Army Rotor System Research Aircraft (RSRA) project is one formally logged system safety program. The executive summary from NASA Contractor Report 3534, "A System Safety Model for Developmental Aircraft Programs," provides an overview of how the RSRA Project Manager/Chief Engineer viewed system safety and applied the concept in the development of this research aircraft. The executive summary is contained in Appendix A. In the words of the RSRA Chief Engineer,

> The fact that the project matured effectively and without incident is believed to be a direct result of the breadth and depth of safety planning and the in-depth involvement of all hands in the safety plan implementation. The point is that the energies devoted to safety tasks are not all penalties to be suffered out of the need for safety; these efforts produce benefits that enhance operational efficiencies, safety aside. [Ref. 9:p. 3]

Cases have also been reported where system safety recommendations were not allowed--and an accident occurred. For example, a project manager decided to eliminate a "roll-over" fuel valve in a helicopter crashworthy fuel system on the grounds of cost savings only to have it reincorporated after an accident demonstrated the need for it. In a similar instance, a change was made to an airplane for value

engineering reasons without system safety review, and the changed configuration produced an accident. [Ref. 2:p. 1-5]

System safety engineers currently use terms such as "increased safety" or "improved safety" concerning the mission performance of a system. The difficulty with these terms is measuring the increased or improved safety of a system. Safety is, in reality, a characteristic such as reliability, maintainability, or supportability, but harder to quantify or measure. Yet, it should be pointed out that these other fields (e.g., reliability, maintainability, and supportability) play major roles in contributing to the overall effectiveness of system safety. For example, an aircraft that has fewer maintenance problems and is easier to maintain has less chance of accidents/mishaps occurring.

Even though System safety is hard to quantifiably measure, it has evolved as a highly technical discipline employing a variety of safety engineering and management tasks. These tasks include the preparation of accident prevention plans and a variety of hazard analyses. Numerous non-engineering system safety tasks (e.g., identification of requirements, accident/incident investigation, feedback of lessons learned, etc.) are also necessary for an effective program. Thus, operations and management skills integrated with engineering talents are the principal components of a system safety program.

Aircraft weapon systems developed prior to the advent of system safety military requirements were usually based on an after-the-fact philosophy of accident prevention. The fly-fix-fly approach: build it and fly it, if it doesn't work, fix it and try flying again. When an accident occurred, an investigation was conducted to determine what was the cause. If the cause was serious and could happen again in the future, system modifications resulted, i.e., engineering change proposals, which are costly and can take several years to implement.

With the advent of the system safety concept came a planned, disciplined, systematically organized, and before-the-fact process characterized as the identify-analyze-control method of safety. An acceptable safety level is designed into the system prior to actual production or operation of the system by requiring timely identification and evaluation of hazard(s)--an implied threat or danger--before losses occur. These hazards are eliminated or controlled to an acceptable level to provide a system that can be developed, tested, operated, and maintained safely.

Safety in a system may, therefore, be defined as a quality of a system that allows the system to function under predetermined conditions with an acceptable minimum of accidental loss. [Ref. 6:p. 8] Yet, system safety is a discipline where successes are usually not evident or documented but where failures are highly visible; i.e.,

loss of life, major aircraft mishap, or severe design deficiencies causing serious mishaps). The measurability and poor documentation problems surrounding the system safety concept can be traced back to 1972 in an Army Safety Center Technical Report 72-8, "Preparation of a System Safety Program Plan for Aviation Systems Development," which states:

> MIL-STD-882 gives the general requirements for System Safety Programs. Army experience in attempting to apply the provisions of MIL-STD-882 directly in aircraft development programs has indicated that there is significant gap between the requirements as stated in the standard and practical, realistic system safety programs. The statement of philosophy and theory of the System Safety concept in the standard and other literature alone are insufficient to produce adequate system safety programs for aircraft development. [Ref. 4:p. ia]

Even today, MIL-STD-882B isn't considered as an all-encompassing document that ensures system safety requirements will be fully implemented. According to Mr. Jim Nerrie, NAVAIRSYSCOM's System Safety Coordinator (AIR516C),

> MIL-STD-882B is basically a generic document which must be tailored to each program and by itself as a contractural document doesn't ensure a program will have a successful system safety effort. It requires more than that. The contractor must have trained system safety personnel and dedicated management support to ensure identified hazards are eliminated not just given lip service. Furthermore, the government i.e., more specifically program managers and systems engineering professionals, must also be concerned with system safety programs requirements. Without government oversight or program office support, the contractor will not fully support or properly implement system safety program requirements.

Mr. Nerrie's comment is further supported by a McDonald Douglas System Safety engineer who stated: "System Safety engineering requirements must be supported by the

government's program manager. If the program manager feels system safety is an important task so will others within the contractor's facilities." He also noted that Air Force program managers seem to place more importance on system safety issues, i.e., known identified hazards needing program management resolution, than Navy Program Managers do.

The 1972 Army report also reported that:

> The System Safety Program Plan (SSPP) must be prepared and used as a contractually binding document. If an SSPP is written from this point of view, it will preclude the incorporation of excessive discussions on theory and philosophy. An SSPP is basically a management proposal for an activity which, when approved, can be directly implemented to produce tangible benefits in a program. Consistent with the extent to which the Systems Engineering Process is formalized in a given project, the System Safety Program Plan should be an essential, integral element of that process. One of the advantages of doing this, from a management point of view, is the use of measurement techniques, employed by Systems Engineering to show the progress in achieving certain objectives in the program. System Safety can to a large extent, be incorporated in such a technical performance measurement system. When fully developed, a useful tool is then provided that can measure and evaluate results obtained in the System Safety Program, something that is difficult to do at present. [Ref. 4:p. 3]

Revision B of MIL-STD-882B doesn't specifically state that an SSPP must be submitted with the contractors proposal. It does state that an SSPP "may be" submitted with the contractor's proposal and "be subject to" contract negotiation, and upon approval by the managing activity, be attached to the contract, referred in the statement of work, and become the basis for contractural requirements. Even though the MIL-STD-882B doesn't specifically state that a

SSPP be a specific requirement prior to source selection, most current aircraft programs do selectively apply Task 101, System Safety Program Plan, in contract-definitized procurements, i.e., requests for proposals and statements of work.

The Army technical report makes a valid point regarding the gap between the requirements as stated in the standard and practical, realistic system safety programs. A main reason for this gap is more than just the practical application of the system safety concept but that system safety doesn't lend itself to any obvious operational measurement; i.e., maintenance man-hours, mean-time-between-failures, or mean-time-to-repair. Technically, this is probably the biggest reason the system safety concept has had severe setbacks in the weapon system acquisition process--i.e., "It doesn't lend itself to any obvious measurement."

B. HISTORY OF SYSTEM SAFETY

One of the first public utterances on behalf of System Safety occurred when Bill Steiglitz of Fairchild Aviation gave a paper titled "Engineering for Safety" to the institute of Aeronautical Science in September 1974. In it he stated the following: "Safety must be designed and built into airplanes, just as are performance, stability and structural integrity. A safety group must be just as

important as part of the manufacturer's organization as are stress, aerodynamics or a weights group." [Ref. 8:p. 103]

In 1969, the Department of Defense revealed that its losses in Southeast Asia alone, up to 31 December 1968, were 1246 fixed-wing aircraft and 982 helicopters through enemy action and 1247 fixed-wing aircraft and 1293 helicopters in accidents. The total cost of losses due to accidents was approximately $2.5 billion [Ref. 10:p. 4]. It is important to note that this figure pertains only to the hardware cost of losses, and doesn't include other costs due to losses such as the value-of-lives-lost, disposal/clean-up costs, or aircraft replacement costs.

During the 1960's, the Department of Defense presumed that a typical aircraft acquisition program for a training command squadron would require 18 aircraft. [Ref. 10:p. 4] A group of 12 squadrons would then need a total of 216 aircraft. An attrition allowance of 3.06 aircraft over a five year period would indicate that 33 aircraft would be lost in accidents and need to be replaced. Assuming this was a fighter-attack aircraft costing approximately $6 million, attrition costs would be $198 million over that time period. If one therefore, avoided the loss of one aircraft a year over this five year period, the savings would total $30 million in 1960 dollars. In current dollars, the cost of fighter/attack aircraft is in excess of

$24 million, so the savings today would actually be four times as great.

It is ironic that avoiding aircraft losses and costs <u>are not</u> the reason behind the military first requiring weapon systems to have system safety. It was more of a concern with unmanned systems, the intercontinental ballistic missiles (ICBMs), that led to the development of the system safety concept. The philosophy with aircraft was that a pilot was a daring individual who lived with hazards because he not only liked to but he had to. Hazards due to failures were common but pilots were usually successful in overcoming these aircraft mishaps. Designers devoted much time to developing emergency procedures and equipment to be used by pilots when failures occurred. The following are examples of preventive measures taken by the designer or methods engineer concerning pilot error prevention through design.

Causes of Primary Errors:

1. Failure to follow prescribed procedures
2. Failure to note critical indication
3. Lack of awareness of hazards
4. Lack of understanding procedures.

Preventive Measures:

1. Ensure that procedures are not hazardous or awkward
2. Provide suitable auditory or visual warning device that will attract operators attention

3. Provide warnings, cautions, or explanations in instructions

4. Ensure that instructions are easy to understand.

With the advent of the ballistic missile, there would be no pilot on board if there was an accident in flight. Designers had no one to devote time to for developing emergency procedures or equipment.

In the early 1960's, the Space Division, then the Ballistic Missile Division was engaged in the operational testing and site activitation of our first ballistic missile systems. During this testing, they lost five CBM's silos, at least five people, and had an extremely low launch-success rate. The significant factor, prevalent in a large percentage of these incidents, was that causes could be traced to deficiencies in design, operational planning, and ill-conceived management decisions. It became apparent that accident prevention lay in the production and design of the missile. Safety problems could only be solved by good design. [Ref. 5:p. 1-1]

In April 1962, the Ballistics System Division of the U.S. Air Force Systems Command produced their Exhibit 62-41, "System Safety Engineering for the Development of Air Force Ballistic Missiles." This document established system safety requirements for the Associated Contracts on the Minuteman Missile. This was the first formal system safety effort. [Ref. 8:p. 103]

In September 1963, the document was revised into Air Force specification MIL-S-38130, "Military Specification-General Requirement for Safety Engineering of Systems and Associated Subsystems and Equipment." With very minor revision, in June 1966, this specification was made a DOD requirement, MIL-S-381308A. Finally, in July 1969, the specification was revised further and became MIL-STD-882, "System Safety Program for Systems and Associated Subsystems and Equipment." Requirements for DOD approval of MIL-STD-882 then became mandatory for a system safety program on all procured products and systems. [Ref. 6:p. 12]

Even though DOD has directed that all DOD procured products and systems have a system safety program, a study done by the Logistics Management Institute in 1984 stated:

> The Office of the Secretary of Defense could not effectively discharge its responsibilities under existing system safety policy instruction (DODINST 5000.36) due to the lack of authorized positions for qualified personnel. There were no experienced system safety professionals in either the Office of the Assistant Secretary of Defense (Manpower, Reserve Affairs and Logistics (OASD (MRAL)) or in the office of the Under Secretary of Defense for Research and Engineering. The responsibility for system safety in OASD (MRAL) is assigned to the Office of Safety and Occupational Health Policy under the Deputy Assistant Secretary of Defense for Equal Opportunity and Safety Policy. The logical basis for the organizational combinations of responsibilities for equal opportunity and safety policy is obscure. Further, the Office of Safety and Occupational Health Policy is erroneously perceived as a social program, legislatively mandated by the Occupational Safety and Health Act, rather than a management function directed at the conservation of high value-resources. This, in turn is a symbol of a lack of top-management understanding of and interest in system safety. [Ref. 2:p. vi]

In summary, the Naval aviation community has had longter, decreases in major aircraft mishaps. Can these decreases be attributed to having an effective system safety program? The F/18 program ahs had an extensive system safety program and currently has an attrition rate much lower than had been expected or planned. Yet, within Naval Air Systems Command current and future aircraft programs are having fewer dollars and manpower resources expended on system safety when compared to the F/18 system safety effort. The need to save a few dollars now is ultimately costing millions of dollars and lost lives in the future. The current trend concerning system safety activities in the Navy demonstrates a need for more support at the levels of Chief of Naval Operations and Commander, Naval Air Systems Command.

III. SYSTEM SAFETY PROGRAM REQUIREMENTS

The first section of this chapter reviews system safety program requirements in the development of a weapon system. In discussing these requirements, emphasis is placed on the importance of the role of the managing activity[1] (MA). The MA has overall responsibility for implementing an effective system safety program.

The second section gives the Department of the Navy's system safety objective along with examples of several sub-objectives contained in MIL-STD 882B. System safety objectives help to provide a balance between identified risks/hazards and the controls necessary to reduce or eliminate them.

The final section provides a logical approach to follow in obtaining system safety objectives. The intention of this section is to provide a logical understanding of how a system safety effort goes about identifying, and eliminating, reducing and/or controlling hazards in the development of a weapon system. Note the importance of "lessons learned." Not only are lessons learned important to begin the system safety process in the development of a

---

[1]Managing activity--the organizational element of DOD assigned acquisition management responsibility for the system, or prime or associate, contractors or subcontractors who wish to impose system safety tasks on their suppliers.

new weapon system but also to end the system safety process in guiding the development of future weapon systems.

A. THE ROLE OF THE MANAGING ACTIVITY (MA) IN ESTABLISHING A SYSTEM SAFETY PROGRAM

The principal objective of a system safety program within DOD is to make sure safety, consistent with the mission requirements, is designed into systems, subsystems, equipment and facilities, and their interfaces.

Yet, the degree of safety achieved in a system depends directly on the managing activity. The managing activity is responsible for determining what definitized statements concerning system safety are written into contractual requirements. His role is also to require that emphasis be given to safety during the system acquisition process and throughout the life cycle of each system, ensuring mishap risk is understood and risk reduction is always considered. Early hazard identification and elimination or reduction of risk to a level acceptable by the managing activity is the principal contribution of an effective system safety program.

MIL-STD-882B has provisions that assist in establishing an effective system safety program effort; but in order to do this, the managing activity must first establish, plan, and implement a system safety program. The responsibility and functions of those directly associated with enforcing system safety policies and program implementation should be

clearly defined, making that sure that all safety inputs to program milestones and reviews are made.

Ensuring this compliance requires that tailored system safety requirements be specified in contractual provisions including the statement of work bidder's instructions, Contract Data Requirements Lists, general and special contract provisions sections, annexes, and other contractural means. The System Specification must also be thoroughly reviewed for inclusion of lessons learned from previously documented safety requirements.

The MA is responsible for choosing those tasks from MIL-STD-882B which should be imposed under contractual agreements keeping in mind at all times that each task produces an extra cost to the program. If a task is not absolutely essential it should not be included. If a task is only partially needed, it should be evaluated to ascertain whether it should be either included in total or tailored so as to require only the element of the task that is essential to the program.

The following is a capsulated summary of the rationale for each task contained in MIL-STD-882B [Ref. 8:pp. 9-12]:

Program Management and Control Tasks

TASK 100--Required to initiate the entire program. Must be carefully tailored, especially for small programs.

TASK 101 - The contractor's 'battle plan.' This not only tells the MA how the contractor is planning to run his safety program, but, because it was prepared by the contractor safety personnel and signed by the contractor

management, the System Safety Program Plan is the safety group's license to operate.

TASK 102--Needed to bring together the safety activities of subs, associates and integrators. If there is but a prime contractor, this Task is not required.

TASK 103--Establishes a requirement for the contractor to present system safety program reviews which formally report hazard analyses and other contractor requirements.

TASK 104--Provides for establishment of special safety groups and System Safety Working Groups.

TASK 105--This task if of utmost importance because it establishes a requirement for closing out hazard action items.

TASK 106--Establishment of a Test & Evaluation program. Needs to be done early in the program!

TASK 107--"When," "What" and "Who to" for progress reports.

TASK 108--Are there to be minimum qualification requirements for System Safety personnel? If so, the requirements are set forth in this task.

Design and Engineering Tasks

TASK 201--Preliminary Hazard List. The first look at potential hazards. Some of the items on this list may later prove to be of little concern. Additional hazards will be considered as the program progresses.

TASK 202--Preliminary Hazard Analysis (PHA). Document in accordance with DI-SAFT-80101, System Safety Hazard Analysis Report. The format for the PHA may or may not be specified by the MA.

TASK 203--Subsystem Hazard Analysis (SHA). Document in accordance with DI-SAFT-80101, System Safety Hazard Analysis Report. The format needs to be the same for the prime and all subs, associates, et cetera. Usually a matrix format for reporting.

TASK 204--System Hazard Analysis. This document interfaces 'safetied' subsystems.

TASK 206--Occupational Health Hazard Assessment. Document as with hazard analyses. Toxicity, hazardous materials and their waste, handling of hazardous items, protective

clothing and devices. Document in accordance with DI-SAFT-80106.

TASK 207--Safety Verification. Were the requirements, specifications, standards, regulations, and guidelines observed and met? Document with DI-SAFT-80102, System Safety Assessment Report.

TASK 208--Training. How is training to be performed and who is to be trained. Details are contained in the System Safety Program Plan.

TASK 209--Safety Assessment. Use DI-SAFT-80102, Safety, Assessment Report which lists and discusses residual safety problems, special controls and procedures.

TASK 210--Safety Compliance Assessment. Document with DI-SAFT-90102, Safety Assessment Report. Wrap-up verification of the safety status of the completed system. On a low-risk system, this may be the only analysis report.

B. SYSTEM SAFETY OBJECTIVES

The Department of the Navy's System Safety Objective as stated in OPNAVINST 5100.24A is:

The objective of a system safety program is to improve operational readiness and reduce costs by using system safety design and analysis techniques.

The Naval Air Systems Command System Safety Objective as stated in NAVAIRINST 5000.3B is:

To identify hazards induced by design, design anomalies, proposed operational and maintenance procedures, and personnel errors sufficiently in the acquisition process to permit resolution prior to the end of full scale development.

System Safety Program Objectives as stated MIL-STD-882B are:

The system safety program shall define a systematic approach to make sure:

a. Safety, consistent with mission requirements are to be designed into the system in a timely, cost effective manner.

b. Hazards associated with each system are to be identified and then evaluated and eliminated or the associated risk reduced to a level acceptable to the MA throughout the entire cycle of a system.

c. Historical safety, including lessons learned from other systems, are to be considered and used.

d. Minimum risk is to be sought in accepting and using new designs, materials, and production and test techniques.

e. Actions are to be taken to eliminate hazards or reduce risks to a level acceptable to the MA.

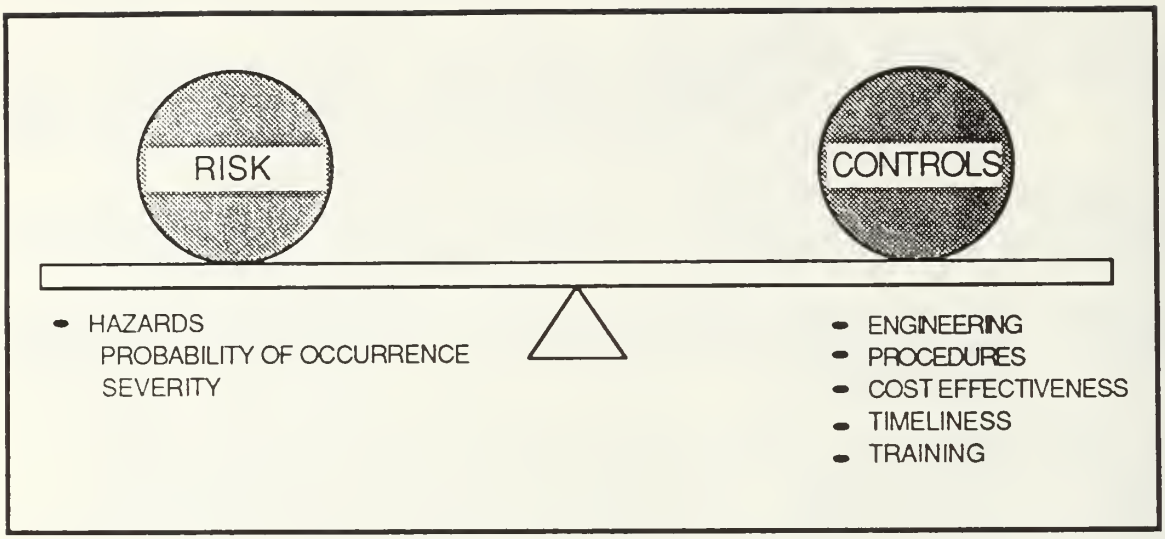
f. Retrofit actions required to improve safety are to be minimized through the timely inclusion of safety features during research and development and acquisition of a system.

g. Changes in design, configuration, or mission requirements are to be accomplished in a manner that maintains a risk level acceptable to the Managing Activity.

h. Consideration is to be given to safety and ease of disposal and demilitarization of any hazardous materials associated with the system.

i. Significant safety data are to be documented as "lessons learned" and submitted to data banks or as proposed changes to applicable design handbooks and specifications.

System Safety objectives can be thought of as producing a balance between risks and controls to eliminate/reduce all identified hazards. [Ref. 6:p. 17] The job of producing this balance is risk management and is illustrated in Figure 3-1 in which risk factors are weighted against controls required to balance those risks:



Source: [Ref. 6:p. 17]

Figure 3.1 Risk Management Control Model

System Safety controls are engineering practices which should be performed such that mission requirements are met in a cost-effective manner with the overall goal being the formation of an accident prevention program for the total weapon system. This entails not only performing system safety engineering practices but developing operational safety controls and participating in accident/incident investigations.

In this context, a system safety program is oriented in terms of program management as well as design or development task performance. It examines the interrelationships of all

components of a program and its systems with the objective of bringing mishap risk or risk reduction into the management review process for automatic consideration in a total perspective. Most important it verifies implementation and effectiveness of hazard control. What is generally not recognized in the system safety community is that there are no safety problems per se in system design. There are only engineering and management problems, which if left unsolved, can result in a mishap. When a mishap occurs, it then is considered a safety problem. Identification and control of mishap risk is then an engineering and management function. [Ref. 5:p. 1-2]. Note the thrust of this statement: system safety is equivalent to mishap risk management. Fundamental to mishap risk management is the requirement that competent and responsible safety management be assigned with sufficient authority so that there is a continuous safety overview of the technical and management planning aspects of the entire program. Keeping in mind that the ultimate responsibility of preventing a mishap belongs to the Program Manager who in essence is the MA.

C. THE SYSTEM SAFETY PROCESS

Although there may appear to be some mystical steps in performing system safety, the system safety process is a logical, engineering approach for obtaining the system safety objectives required by the managing activity. [Ref. 10:p. 109] The steps of this process can be followed in

sequence at any level of system complexity without destroying the basic idea. The process is repeated as necessary during the system life cycle. What follows is a step-by-step explanation of the System Safety Process as applied to any system.

The System Safety Process can begin at any point in the life cycle of a system, but its greatest advantages are achieved when it is first applied very early in the cycle. It is not too early to begin applying the process during initial concept studies which will ultimately lead to the production and use of a system. [Ref. 4:p. 34] The system safety process consists of the following steps.

1. Lessons Learned

The process begins with the review of Lessons Learned from previous weapon systems. This represents the sum total of experience and knowledge gained from previous operations of systems related to the one under consideration. This experience and knowledge will rarely exist in any one place, so the effectiveness of the remainder of the process will depend on the ability to concentrate pertinent information at the point required for its use. Of particular interest are those measures taken previously to correct design features which have resulted in injuries and deaths or accidental damages and losses. Design features which have not proven unacceptably hazardous are also included here. Thus, the process logically begins

with the identification and collection of pertinent information.

2. System Specifications/Delineation

The design of any new system must be predicated on the definition of the system and its bounds. The second step in this process is to clearly state just what system is under consideration. Any entity can be labeled a "system" as long as it is accurately defined. The boundaries of the system and its elements must be defined as early as possible and revised as required during the system life cycle. Included in this area is the definition of the system operating condition, environmental situation, and the human role in system operation. Such delineation establishes the limits for succeeding steps in the process and reduces complex systems to manageable parts. For instance, if an aircraft system is being considered, it is essential to know whether the crew is being thought of as part of the system or not. Careful attention to this step prevents confusion later in the process.

3. System Hazard Analyses

The heart of the System Safety Process is the analysis of a system and its elements in a comprehensive and methodological manner. Beginning with the Preliminary Hazard Analysis (PHA) of the design concept and continuing through the System Hazard Analysis (SHA) of the complete system, this analytical process utilizes various techniques

to systematically examine the system for potential hazards. The detailed methods and techniques for performing these analyses are selected based on their suitability for the particular system element under consideration and the applicable level of detail in the design. It is in this step that before-the-fact accident prevention has its beginning. The key to doing this lies in the comprehensive and methodical approach to analysis. By comprehensive, it is meant that everything which could happen to the system is thought of in terms of the consequences which may result. The analyst continually asks the question, "What if such-and-such happens?" To do this without getting hopelessly bogged down in complex details requires a methodical or systematic approach to the analysis. Many analytical tools for this are available and in use today. The result is a high degree of confidence that no stone has been left unturned in the search for possible system hazards.

4. Hazard Identification

Through the systematic hazard analyses described in the previous step, the designer or engineer identifies those features of a system which potentially may cause injury, damage, or destruction. The primary reason for going through the analysis is to arrive at this step. A hazard must be identified before it can be eliminated or controlled. As the design progresses, additional hazards

may be identified during successive iterations of the System Safety Process.

5. Hazard Categorization and Evaluation

To eliminate every hazard identified in the previous step is usually going to be impractical. For example, analysis of a helicopter system will show that separation of a rotor mast is a hazard with catastrophic consequences. As a result, we can make the mast stronger or more reliable, but we can neither eliminate the hazard nor give 100 percent assurance that it will never fail. Similar situations arise in examining the role of the human in a manned system. It is unlikely that we will ever totally eliminate his potential for making mistakes. A procedure is developed by which hazards identified through the analytical process can be categorized and evaluated for the purpose of enabling decisions to be made with regard to appropriate corrective action. The following criteria should be used in developing this procedure:

- Hazards are evaluated to determine the worst potential consequences which would ultimately occur if the hazard is not eliminated or controlled.
- Consequences or effects of hazards are expressed in terms of their impact on mission effectiveness, their effect on personnel and materiel failure or malfunction.
- Effects on personnel and material are classified to levels or degrees of severity.
- The probability of hazard manifestation under the various operating conditions is determined.
- The resources of penalties required to eliminate or control an identified hazard are determined in terms of

cost (dollar value of policy procedure revisions, manpower, technology, facilities, materiel, etc.) schedule, and system performance.

A means by which identified hazards can be arranged in order of priority for corrective action is developed. It is here that judgement must be applied to ensure that maximum practical benefits are derived from this process. Responsibility for accomplishing this step is usually vested in the management of a system program as an essential element in the decision-making process necessary to identify alternatives and to implement appropriate corrective action.

6. Action(s) to Eliminate or Control Hazard(s)

Nothing that has been done so far in the system safety process will prevent the first mishap. The process produces no useful result until some action is actually taken to eliminate or control the hazards that have been identified. Without proper and timely action, the process becomes ineffective. However, all steps taken up to this point have been designed so that the most appropriate action can be taken. Again, management is responsible for this step. This responsibility includes the decision and direction for action, plus the allocation of resources required to do the job. This is perhaps the most crucial step in the entire process because it is here that practical results are actually achieved.

7. Modification of System Element(s)

Any action taken in the previous steps will result in the modification of some element or elements of the system. This modification need not only involve hardware. For example, procedures can be revised, initial assumptions on operating environment can be amended or basic specifications can be changed. Since action modifies the system, the initial definition of the system or its elements also change, so the delineation of the system in step B must be revised accordingly. The process is then repeated, as required, until such time as no unacceptable additional hazards are generated by the system modification. These repetitive steps ensure that actions taken to correct one hazard do not induce other hazards somewhere else in the system.

8. Effectiveness Evaluation of Action Taken

Up to this point in the process, hazards identified in the system through analysis have been eliminated or controlled within practical program limitations. If the technology of today were able to give up 100 percent assurance that we were 100 percent correct in all we have done so far, the process could end here. Since we cannot give these assurances, some measure of effectiveness is needed. Effectiveness is evaluated against the extent to which the system safety objective has been attained. A

satisfactory evaluation results in increased assurance in the level of safety of the system.

9. Accident Incident Analysis

The occurrence of an accident or incident, of course, leads to an unsatisfactory effectiveness evaluation. In this step, any mishap is examined critically to determine causes and evaluate effects. The causes and effects could range from something already predicted as possible, or even probable under certain circumstances, to something entirely new and surprising. The results of this mishap analysis should then reveal deficiencies in the System Safety Program and serve to direct corrective action back to the appropriate step in the process. In this way, maximum use is made of the mishap experience, without having to go back and continually rediscover new truths.

10. Component/System Test and Demonstration

The inadequacy of analytical techniques alone in identifying all system hazards is determined in step H. Most, if not all, development programs for complex systems include testing to verify performance and the demonstration of system capabilities. Both of these activities are, in essence, assuring functions. They are conducted to assure the user that his system performs as it is supposed to. System safety is also an assumption. Tests and demonstrations normally performed on a system or its components are planned and conducted to reveal inadequacies

in the System Safety Process. At the same time, these tests and demonstrations serve to verify the results of the process and give greater confidence in the assurances provided. As with the results of mishap analyses, deficiencies uncovered in this step are directed to the appropriate step in the process for corrective action.

11. Increased Safety Assurance

In those areas where the effectiveness evaluation (Step 5) and test and demonstration (Step 7) indicate that the System Safety Process has produced the desired results, assurance that the system safety objective has been met is increased correspondingly. This increased assurance is then applied the next time we go through the process, an element of system qualification, or in applying the process to another system. In this manner, we continually build on past processes, while simultaneously correcting deficiencies.

12. Final Step

The final step is to document whatever new lessons learned were developed so that they will be available for consideration in future systems. [Ref. 4:pp. 34-37]

This is the System Safety Process. At first glance, the overall picture may seem complicated and confusing. But when each step is considered individually, a logical and progressive pattern develops. It is really no more than a specialized problem solving process, one step leading

naturally to the next. The System Safety Process also has several distinct characteristics which enable it to be applied in a practical manner. Provisions are made to repeat the steps as often as necessary to achieve the desired results. There are no blind alleys. The process can be applied at any level of system complexity, from broad general design concepts to the final details of a subsystem. Another significant practical characteristic of the process is that is prescribes the application of judgement and management decisions at the juncture between what is ideal and what is practical. Thus, the System Safety Process produces results which are consistent with the definition of system safety, attainment of an ". . . optimum degree of hazard elimination within the constraints of operational effectiveness, time and cost." [Ref. 4:p. 37]

Actually, the applications of the System Safety Process is not simple. But neither is a sophisticated weapon system simple. The advantage of the process lies in being able to examine such extremely complex subjects in simpler related parts. This examination proceeds in a logical and orderly fashion from one part to the next until the entire complex subject is covered. [Ref. 4:p. 37]

IV. COST-BENEFIT ANALYSIS OVERVIEW

> Benefit-cost analysis, when used as a central element in making certain public investment decisions, forces careful consideration of problem identification, solution comparisons, and the specific impacts and opportunity costs associated with the investment of public funds.
> James J. Goshling and Lowell B. Jackson

The process of identifying acceptable public projects has become identified with the term benefit cost analysis (BCA). The purpose of this chapter is to discuss the fundamental concept of BCA. The chapter will:

a. define benefit-cost analysis

b. define cost-effectiveness analysis (CEA)

c. provide a historical overview of benefit-cost analysis

d. review provisions of Executive Order 12291--Federal regulatory requirements regarding BCA

e. end with an assessment of the difficulties involved in doing a BCA/CEA on safety related issues.

A. DEFINITION OF BENEFIT-COST ANALYSIS

Among noneconomists, "benefit-cost-analysis" and "cost-effectiveness analysis" are often considered to be "techniques" for appraising public projects. A "cost-effectiveness analysis" is considered to be a special form or subset of BCA distinguished by the difficulty with which project benefits can be identified in terms of dollars. Peter Sassone and William Schaffer define a benefit-cost analysis as an "an estimation and evaluation of net benefits

associated with alternatives for achieving defined public goals." [Ref. 11:p. 2]

J.D. Bentkover states, "Benefit-cost analysis has, in many policy contexts, been considered any analytical method that enumerates the advantages and disadvantages of alternative actions." When interpreted in economic terms, it is a pragmatic realization of the theory of welfare economics, providing a specific organizing framework and a set of procedures to summarize information and display tradeoffs associated with these actions--generally in monetary terms. In more stricter economic considerations, BCA judges actions strictly on an efficiency criterion. A positive aggregation of net benefits implies the prospects for improvement in resource allocation. [Ref. 12:p. 13]

Cost-benefit analysis as a generic term embraces a wide range of evaluation procedures which leads to a statement of assessing costs and benefits relevant to project alternatives. The variety of problems addressed and the ingenuity which must be exercised in existing costs and benefits make it particularly difficult, if not impossible, to design an all purpose BCA procedure. Several general principles may be stated, but an all-encompassing procedure cannot be defined. [Ref. 11:p. 3]

The basic notion of BCA seems to be simple. If we have to decide whether to do A or not to do A, the rule is: "Do A if the benefits exceed those of the next best alternative

course of action, and not otherwise. If we apply this rule to all possible choices, we will generate the largest possible benefits, given the constraints in which we live."

Going one step further, we must consider the "benefits of the next best alternative to A." The alternative benefits to A will then be labeled to the "costs of A," for if A is done the alternative benefits are lost. The rule is: "Do A if its benefits exceeds its costs, and not otherwise."

The concept of BCA so far seems quite simple, yet, problems arise in measuring the identified benefits and costs, and then justifying why project A is better than project B. There must exist some means of comparing the various dimensions along which A and B differ.

Some people believe that one particular attribute of life, such as silence of the countryside, is of absolute importance. For them cost benefit analysis is easy: the value of all other benefits and costs is zero. More problematic are those people who believe in the absolute importance of two or more items, for them they are doomed to intellectual and spiritual frustration. Whenever A is superior to its alternative on one count and inferior on another, they will be obliged to do both. Unfortunately, choices between such alternatives have to be made only too often and its impossible to make rational choices unless every item has a unique price. Its sufficient to know that

the price lies within some range, the answer will be unaffected by having an exact price. The basic principle is that we assign numerical values to benefits and costs, and arrive at decisions by adding then up and accepting those projects whose benefits exceed their costs. [Ref. 13:p. 10]

How are these values to be arrived at? If only people matter, the analysis would involve the following two steps:

1. How does the decision affect the welfare of each individual concerned? To judge this effect you must rely on the individual's own evaluation of his mental state and then measure his change in welfare as he himself as he himself would value it; i.e., What would he be willing to pay to acquire the benefits or to avoid the costs. These costs don't have to be in monetary terms.They could well be bottles of beer. Yet the problems of inferring people's values from their behavior are clearly made and illustrate the central problem in doing a BCA. [Ref. 13:p. 10]

2. How do you deduce the change in social welfare implied by all changes in individual welfare? Unless there are no losers, this means somehow valuing each man's welfare. If incomes were optimally distributed, each person's welfare would be equally valuable regardless of whose it was, which means that each man's welfare has equal weight. If incomes are not optimally distributed, economists argue that it should be redistributed by cash transfers rather than through the choice of projects. But what if welfare cannot be redistributed, even if it should be; the poor man's welfare may need to be valued more highly or have more worth than the rich man's welfare. [Ref. 13:p. 10]

This raises the question that underlies almost all disputes about BCA: Which constraints are to be taken as given? And what about the constraints outside the realm of the decision-maker? This brings us to the relationship between BCA and public policy. The government's overall aim is presumably to ensure that social welfare is maximized:

subject to those constraints over which it has no control; i.e., such as tastes, technology and resource endowments. In any economy this objective requires some government activity owing to the failure of free markets to deal with the efficiency problems of externalities; economies to scale, inadequate markets of risky outcomes, and the equity problem of the mal-distribution of wealth. [Ref. 13:p. 11]

The great strength of BCA is that it permits decentralized decision-making. This is needed because no one public office can hope to handle the vast mass of technical information needed to decide on specific projects. But yet it requires the assumption that right decisions will only result if the prices used by the decision-maker reflect the social values of input and output at the social optimum, or what are usually called their "shadow prices." [Ref. 13:p. 9] In a mixed economy, market prices often do not do this. This poses another problem in doing a BCA; i.e., to arrive at adequate and consistent valuations where market prices fail. If any of the activities of government agencies are non-optimal then another problem arises in doing a BCA, i.e., the difficulty in finding relevant prices, namely whether and how to allow for those divergences between market prices and those social values that arise from the action or inaction of government itself. [Ref. 13:p. 12]

Edward Gramlich wrote of BCA that "ultimately, it is nothing more than a logical attempt to weigh the pros and cons of a decision. And ultimately, something like it must necessarily be employed in any rational decision." [Ref. 14:p. 3] James Campen states that "this injunction that one should undertake a proposed action if and only if its advantages (benefits, pros) outweigh its disadvantages (costs, cons) is without practical content." Campen's concern is with BCA as a systematic, quantitative approach to the comparative evaluation of governmental expenditure and regulatory alternative. [Ref. 15:p. 15]

With this in mind, the goal of BCA is to identify the alternatives that will make the most efficient use of society's scarce resources in promoting social objectives, that is--that will provide the maximum net social benefits. A BCA is carried out from a social or public point of view rather than from the private, profit oriented perspective that guides the financial analyses undertaken by firms or individuals; it attempts "to take account of all of the effects of a project on members of the public, irrespective of who is affected and of whether or not the effect is captured in a financial account." [Ref. 16:p. 24]

There is a spectrum of views of the nature of "Decision Makers," and of the decision-making process. One end of the spectrum envisions decision-makers commissioning BCA's and then taking their results into account in making more or

less unilateral decisions. The other end of the spectrum sees benefit-costs analysts as providing inputs to a wide range of individuals and groups who participate in a pluralistic political process of outcome determination. All along the spectrum, BCA is viewed as an essentially neutral technique for providing helpful input to legitimate and effective decision-makers who function to represent the interests of the entire population and thereby to promote social welfare. [Ref. 15:p. 26] One text states, for example, that "government is really the collective expression of the will of taxpayers" [Ref. 14:p. 26] and another explains that BCA is "carefully designed to ensure that public decisions accurately reflect what it is that the society wants to accomplish" [Ref. 17:p. 26].

One school of thought-called the conventional approach by E.J. Mishan who is its most forceful and persistent advocate--maintains that BCA's, like engineering analyses, ought to be based only on objective, scientifically observable data and generally acceptable principles. In this view the objective of scientifically observable data relevant to a BCA are market data, and the only generally acceptable economic principle for evaluating alternative outcomes is that of economic efficiency, or maximization of total net benefits evaluated on the basis of market data. According to the conventional approach, there should be no

special relationship between decision-makers and analysts. [Ref. 15:p. 26]

The other school for thought--called the decision-making approach by Robert Sugden and Alan Williams, who are its most systematic and persuasive advocates in the texts under review, and labeled "revisionist" by Mishan--maintains that there should be a much closer relationship between decision-makers and analysts. Decision-makers should actively use analysts to obtain information and analysis that will be useful to them in identifying those most productive in reaching their goals. In this view, the analyst serves essentially in a staff role to the decision-maker and an analysis does not stop with "objective" market-based data. [Ref. 15:pp. 26-27]

The conception of the role played by benefit-cost analysis (and analysts) in the process of determining what proposed expenditures and regulations are actually undertaken is a central element of the BCA paradigm. This conception may be summarized by saying that benefit-cost analysts play the role of technicians, providing information and analysis to politically responsible decision-makers. The decision-makers must then somehow combine the information and analysis received from benefit-cost analysts with other considerations in the final process of reaching a decision. As one text puts it: "Sound expenditure decisions, whether made by the legislator or the executive,

require detailed information regarding the merits of alternative projects." [Ref. 15:p. 25] "The technician can perform an important service in providing this information." [Ref. 18:p. 25] Another makes the point this way: "A well-conducted cost-benefit study can be only a part, though an important part, of the data necessary for informed collective decisions." [Ref. 19:p. 25] And a third: "CBA is an 'input,' an 'aid,' an 'ingredient' of decision-making. It does not supplant political judgement." [Ref. 20:p. 25]

BCA shares the public policy perspective of most of current mainstream economics, according to which the major purpose of economic analysis is to contribute to the formulation and adoption of improved public policy. The provision of reasoned arguments, relevant information, and insightful analyses can make a positive contribution to better decisions and hence to improved social welfare. The characterization of the role of BCA that was articulated in a highly influential survey article a quarter of a century ago reflects the view of the BCA paradigm:

> The economist must interpret the desires of the policy people whom he is serving and express them in an analytical form as an objective function. He then seeks to maximize the function, given the empirical relations in the economy and the institutional constraints that may be appropriate to the analysis. In this manner, the economist can play the role of technician, of bringing his technical equipment to bear on policy problems, with maximum effectiveness. [Ref. 15:p. 25; emphasis added]

In conclusion, elements involved in carrying out a BCA are:

- Determining the role of BCA in the overall processes of decision-making and outcome determination: This involves answering such questions as, For whom is the analysis being done? How will it be used on its completion? What conceptions of government and of the political process underlie the BCA paradigm?

- Determining the social goals that provide the basis for the comparative evaluation of proposed alternatives: Costs and benefits can be identified and measured only relative to specific criteria or objectives that determine what is to be maximized. In the jargon of economics, it is necessary to specify an objective function that will provide the basis for valuing costs and benefits.

- Identifying, correctly and comprehensively, the benefits and costs of the proposed alternatives, and then measuring each type of benefit and cost: This involves determining the value of benefits and costs at the time that they occur and for the people directly affected.

- Combining, or aggregating, all of these benefits and costs together in order to determine an overall summary measure of an alternative's net benefits: Three particular types of aggregation are given a great deal of attention by the BCA paradigm: (1) aggregating benefits and costs that occur in different time periods (that is, dealing with the issue of discounting); (2) aggregating benefits and costs that accrue to different individuals or groups of people (that is, dealing with distributional issue); and (3) aggregating circumstances (that is, dealing with risk and uncertainty).

- Reaching a conclusion: This may involve using an appropriate criterion for choosing among proposed alternatives on the basis of their total benefits and costs as determined in the preceding stages of the analysis. More generally, it involves presenting the results of the benefit-cost analysis in a way that is appropriate in light of the first two elements identified here--the role of the analysis in the overall decision-making process and the nature of the objective function adopted for the analysis. [Ref. 15:p. 27]

B. DEFINITION OF COST-EFFECTIVENESS ANALYSIS

> The military effectiveness or military worth of any given weapon system cannot logically be considered in isolation. It must be considered in relation to its cost--and, in a world in which resources are limited, to the alternative uses to which the resources can be put. Military requirements are meaningful only in terms of benefits to be gained in relation to their cost. Accordingly, resource costs and military worth have to be scrutinized together. [Ref. 21:p. 26]

The above quotation perhaps best expresses what "cost-effectiveness" is about--the obtaining of maximum desired benefits at the minimum expenditure of resources.

Regardless of the scale or character of the system to be evaluated, cost-effectiveness in its modern use is concerned with estimation of costs and the evaluation of the worth or effectiveness of systems. To these two considerations, we may add a concern with time.

Cost, according to Webster, is "the amount paid or given for anything hence whatever, as labor, self-denial . . . etc., is requisite to secure a benefit." The important point to keep in mind is that cost is one element of value (or benefit) foregone in order to "secure" a greater benefit. In short, cost is a negative benefit. Cost is not limited to money, but rather it must include all benefits or desired effects which may have to be sacrificed in order to obtain greater benefits. It certainly includes money, time, performance, consumption of scarce resources, and use of available human skills. [Ref. 22:p. 4]

Effectiveness, in contrast, connotes the desirable effects or benefits gained by reason of the expenditure or incurring of a cost. In other words, costs are always trade-offs for expected greater benefits. Effectiveness also connotes some measure of performance or level of output of the benefit-producing system. The benefit of an engineering cost may be an airplane: the level of its performance is the effectiveness. On the other hand the word benefit may also be interpreted to mean not only the generic description of the system but also its measurement. I believe that benefit may be more descriptive than effectiveness, but these words may mean the same thing in relation to an economic evaluation. [Ref. 22:p. 4]

In a military context, a CEA analysis might tackle such questions as the extent to which aircraft should be repaired at a depot rather than on the base; the possible characteristics of a new strategic bomber and whether one should be developed or not; and how much safety should be designed into an aircraft or not. Each stage of analysis involves as one stage a comparison of alternative courses of action in terms of their costs and their effectiveness in attaining some specific objective. This is cost-effectiveness analysis, narrowly defined. Usually it consists of an attempt to minimize dollar cost subject to some mission requirement (which may not be measurable in dollar terms)

or, conversely, to maximize some physical measure of output subject to a budget constraint. [Ref. 23:p. 1]

To qualify as a complete analysis, a study must look at the entire problem in its proper context. Characteristically, such an analysis should involve a systematic investigation of the decision-maker's objectives and of the relevant criteria: a comparison--quantitative where possible--of the costs. Effectiveness, risks, and timing associated with the alternative policies or strategies for achieving each objective.

In defense planning, where there is no accepted theoretical foundation, advice received from experts working individually or as a committee is largely dependent on subjective matter. The advice obtained from a cost-effectiveness analysis should also. The virtue of analysis of any kind is that it is able to make a more systematic and efficient use of judgment than any of its alternatives. The essence of the method is to construct and operate within a "model"--an idealization of the situation appropriate to the problem. Such a model may take many forms. Its purpose is a means of communication, enabling participants in the study to make their judgments in a concrete context. What is important is feedback--the results from the model help the decision-maker, analyst, and other experts on whom they depend to revise their earlier judgments and thus to arrive

at a clearer understanding of the problem and its context. [Ref. 23:p. 3]

The central importance of the model can be seen most readily by looking at its relation to the other elements of analysis. There are five altogether. Each of them is present in every analysis of choice, although they may not always be explicitly identified. [Ref. 23:pp. 4,5]

1. The Objective(s)

Cost-effectiveness analysis is undertaken primarily to help choose a policy or course of action. One of the first and most important tasks of the analyst is to attempt to discover what objectives the decision-maker is, or should be. Trying to attain through this policy, and how to measure the extent to which they are, in fact, attained. This done, strategies, forces, or equipment are examined, compared, and chosen on the basis of how well and how cheaply they can accomplish these objectives.

2. The Alternatives

The alternatives are the means by which it is hoped the objectives can be attained. They need not be obvious substitutes for one another or perform the same specific function. Thus, to build the attack aircraft to perform one mission or several different types of missions or whether to fly 250 knots vice 400 knots are all alternatives.

3. The Costs

The choice of a particular alternative for accomplishing the objective(s) implies that certain specific resources can no longer be used for other purposes. These are the costs. In analyses for a future time period, most costs can be measured in money, but their true measure is in terms of opportunities that they preclude. Thus, if we are comparing ways to prevent mishaps from occurring, each of the various ways has a cost attributed to it.

4. A Model(s)

A model is a simplified representation of the real world which abstracts the features of the situation relevant to the question being studied. The means of representation may vary from a set of mathematical equations or a computer program to a purely verbal description of the situation, in which judgment alone is used to predict the consequences of various choices. In cost-effectiveness analysis (or any analysis of choice), the role of the model is to predict the costs that each alternative would incur and the extent to which each alternative would assist in attaining the objectives.

5. A Criterion

A criterion is a rule or standard by which to rank the alternatives in order of desirability and choose the most promising. It provides a means of weighing costs against effectiveness. [Ref. 23:p. 5]

Having formulated and researched the problem--that is, clarified the issues, limited the extent of inquiry, searched out the necessary data and relationships, and identified the various elements--the process of analysis is complete. Unfortunately, things are seldom so tidy: alternatives are sometimes not adequate to attain the objectives; the measures of effectiveness do not really measure the extent to which the objectives are attained; the predictions from the model are apt to be full of uncertainties, and other criteria which look almost as attractive as the one chosen, may lead to a different order of preference. The key to the successful analysis is iteration--a continuous cycle of formulating the problem, selecting the objectives, collecting the data, building new models, weighing the cost against performance, questioning assumptions and data, reexamining the objectives, opening new alternatives, and so on until satisfaction is obtained or time or money forces cut-off. [Ref. 23:p. 5]

In stating the purpose of cost-effectiveness analysis, it is possible to see what it can and cannot do. It can be applied to a range of problems extending from very narrow to the very broad. Yet, every analysis has defects. Some of these are limitations inherent in all analyses of choice. Others are due to difficulties encountered in coping with such things as the varying times at which alternatives become available or uncertainty about the

future. Still others are flaws or errors, which, hopefully, will disappear as we learn to do better, more thorough, and complete analyses. [Ref. 24:p. 5]

C. HISTORICAL OVERVIEW OF BENEFIT-COST ANALYSIS

Benefit-cost analysis most recently can be traced to Executive Order 12291, issued by President Reagan in 1981. In short, this Executive order requires Federal agencies to perform benefits assessments of proposed major regulations and prohibits them from taking regulatory action unless potential benefits exceed potential costs to society.

Although common-sense principles of benefit-cost analysis have prevailed for centuries, the applications of formal BCA techniques is a twentieth-century phenomenon. On of the first applications occurred in 1902, when the River and Harbor Act directed the Corps of Engineers to access the costs and benefits of all river and harbor projects. More widespread use occurred after the Flood Control Act of 1926, which explicitly required that only projects whose benefits exceeded their costs be submitted for congressional action. (BCA book) Yet, the act itself gave no guidance on the implementation of this criterion. Practice soon developed on the basis of tradition and in which later became known as the "Green Book." The "Green Book" never received official status but was highly influential. Many of the ideas in the book were incorporated in the U.S. Bureau of the Budget's

Budget Circular A-47 which promulgated a set of guidelines for all benefit-cost analyses of water resource projects.

The next important influence on the Concept of BCA took shape during the 1950's, as analysts of the Rand Corporation, under contract to the U.S. Air Force, grappled with the resource allocation problems facing the managers of military spending programs. Although they advocated techniques of systems analysis and cost-effectiveness analysis rather than benefit-cost analysis, many of the core ideas were closely related. An unclassified exposition of the conceptual approach and analytical techniques developed at Rand was provided in Charles J. Hitch and Roland N. McKeans's The Economics of Defense in the Nuclear Age. This book became known as "the Bible of the Pentagon" after newly installed Defense Secretary Robert McNamara made Hitch an Assistant Secretary of Defense and charged him with implementation through out the Defense Department the planning, budgetary, and analytical techniques developed at Rand; BCA like other techniques are one important component of the planning-programming-budgeting system (PPBS) that was put into place at the Pentagon in the early 1960's. [Ref. 15:p. 18]

The 1960's then witnessed a great expansion in the range of spending programs to which BCA was applied. First there were applications to other kinds of physical investment projects such as transportation and urban renewal. These

were soon followed by applications in such areas of social spending as health, education, and income maintenance. A major emphasis to this spreading of BCA was President Lyndon Johnson's August 1965 decision to implement PPBS, based on that of the Defense Department, throughout the civilian sector of the federal government. [Ref. 15:p. 20]

The dramatic wave of "social regulation" enacted in the late 1960's and early 1970's was followed by attempts to use BCA to guide the growth of federal regulatory activity. BCA began to be applied to economic, environmental, and health and safety regulation in addition to public expenditure projects. In response, new criticism and controversy emerged. [Ref. 15:p. 20]

The nature of Executive Order 12291, issued by President Ronald Reagan within a month of his inauguration, was viewed, both by those who favored it and those who opposed it, as part of the new administration's conservative agendas. Few doubted that, to the extent it was actually implemented, the effect would be to reduce social regulation in the areas of health, safety, and consumer protection. Liberal critics denounced BCA for its pro-business bias, viewing it as one more tool for reducing the size and scope of big government.

In 1965, during Johnson's reign, BCA was considered an important part of the Federal government. BCA was then viewed as a tool for guiding the expansion of government

spending and for aiding government planning and management of its economic activities. It was also perceived as a liberal, "good management" measure that would reduce the influence of special interests so that government programs could be more effective in aiding those that they were intended to aid. [Ref. 15:p. 20]

D. PROVISION OF EXECUTIVE ORDER 12291

The effects of Executive Order 12291 were threefold. First, it expanded the definition of "major rule" and so incorporated a greater number of regulations within its purview. Second, it granted the OMB authority to order that a rule not designated major by an agency head may be so designated. Third, it required that any set of related rules be considered together as a major rule. [Ref. 24:p. 2] Executive Order 12291 established the following analytical requirements for major rules:

1. Administrative decisions shall be based on adequate information concerning the need for and consequences of proposed government actions.

2. Regulatory action shall not be undertaken unless the potential benefits to society from the regulation outweigh the potential costs to society.

3. Regulatory objectives shall be chosen to maximize the net benefits to society.

4. Among alternative approaches to any given regulatory objective, the alternative involving the least net cost to society shall be chosen.

5. Agencies are to set regulatory priorities with the aim of maximizing the aggregate net benefits to society, taking into account the condition of the particular industries affected by regulations, the condition of

national economy, and other regulatory actions contemplated for the future [Section 2(a)-(e)].

To implement these analytic requirements, a new process for conducting regulatory impact analysis (RIA) was required. This process increases the time frame for promulgating regulations and specifies that an RIA must contain the following [Section 3(d)(1)-(5)]:

1. A description of the potential benefits of the rule, including any beneficial effects that cannot be quantified in monetary terms, and the identification of those likely to receive the benefits:

2. A description of the potential costs of the rule, including any adverse effects that cannot be quantified in monetary terms, and the identification of those likely to bear the costs;

3. A determination of the potential net benefits of the rule, including an evaluation of effects that cannot be quantified in monetary terms;

4. A description of alternative approaches that could substantially achieve the same regulatory goal at lower cost, together with an analysis of this potential benefit and costs and a brief explanation of the legal reasons why such alternatives, if proposed, could not be adopted; and

5. Unless covered by the description required under paragraph (4) of this subsection, an explanation of any legal reasons why this rule cannot be based on the requirements set forth in Section 2 of this Order.

This constitutes a considerable increase in the nature and amount of substantiation an OMB review requires to sustain regulatory actions. [Ref. 24:p. 3] Moreover, Section 4, "Regulatory Review," requires that before approving any final rule, each agency shall [Section 4(a)-(b)]:

a. Make a determination that the regulation is clearly within the authority delegated by law and consistent with congressional intent, and include in the Federal Register at the time of promulgation a memorandum of law supporting that determination.

b. Make a determination that the factual conclusions upon which the rule is based have substantial support in the agency record, viewed as a whole, with full attention to public comments in general and the comments of persons directly affected by the rule in particular.

With respect to (b), weight must be given to general public comments and then "special" weight must be given to comments of persons directly affected by the rule. This appears to require a balancing of the concerns of both those incurring the costs and those receiving the benefits of the proposed regulations. [Ref. 24:p. 3]

Only three types of regulations are exempt from these procedures: regulatory responses to an emergency situation; regulations for which these procedures would conflict with deadlines imposed by statue or judicial order; and such others as directed by the President's Task Force on Regulatory Relief (Section 8). [Ref. 24:p. 3]

Executive Order 12291 has several implications. Briefly it now requires:

1. Increased time requirements for the proposal, approval, and promulgation of regulations.

2. More rigorous demonstration of the benefits of the proposed actions, to the extent of weighing benefits against the societal cost.

3. Explicit analysis and selection of alternatives with the lowest societal cost.

4. More detailed and substantive analysis to support rule-making.

In order to assist agencies in satisfying the requirements of Section 2 of E.O. 12291, OMB issued regulatory impact analysis guidelines in 1981. These state that RIA's should be written to enable independent reviewers to make an informed judgement that the objectives of E.O. 12291 are satisfied. Specific guidelines for the development of RIAs state that the following be provided [Ref. 24:p. 4]:

1. Statement of need for and consequences of the proposed regulatory action.

2. Examination of alternative approaches, including consequences of having no regulation and alternatives within the scope of the proposed action (e.g., less stringent permissible exposure levels, different effective dates, and alternative means of compliance.)

3. Analysis of benefits and costs including estimates of present value expressed in constant dollars using an annual discount rate of 10 percent; specific type of benefits, when received and by whom; and the type of costs, when incurred and by whom.

4. Net benefit estimates including nonmonetary but quantifiable benefits, nonquantifiable benefits and costs, and cost effectiveness of various alternatives.

5. A rationale for choosing the proposed regulatory action (which should achieve the greatest net benefit to society.)

6. Statutory authority.

The major implication of the OMB guidelines is that RIAs must not only explicitly consider nonregulatory alternatives but must use risk and benefit assessments to link the market

failure causing the problem to the proposed regulation. [Ref. 25:p. 4]

E. DIFFICULTIES OF ASSESSING SAFETY

Benefits that are intuitively felt to be the most important; i.e., health, safety, and the environment, are also among the most difficult to measure. They are not readily quantifiable (e.g. improved quality of life, avoidable aircraft mishaps, enhanced quality of surroundings) or even when units of benefits can be defined, their value in terms of dollars or other standard measures is a matter of subjective judgement. In cases of quantifiable benefits, problems arise when a value is attached not only to the benefit perceived by each individual but also to an equitable distribution of the benefit across a population as a whole. [Ref. 24:p. 8]

The area of safety is specifically concerned with events not only having a probability of occurrence but potentially severe consequences. In conjunction with this, safety is concerned with the adequacy of the safety precautions surrounding such events. In the past, benefit-cost analysis studies of safety focused on the avoidance of risk and the identification of cost-effective risk-reduction measures. [Ref. 24:p. 8] Examples of such risk reduction measures pertaining to safety are:

1. Reduced chances of the release of hazardous material and of the destruction of property.

2. Reduced quantities of hazardous materials if and when a release occurs.

3. Decreased numbers of mishaps involving fatality(ies) or injury(ies).

4. Decreased numbers of expected fatalities or injuries.

5. Decreased property damage or production group of people.

6. Better distribution of risk(s) across a particular group of people.

7. Reduced insurance premiums or avoidance costs.

8. Reduced lawsuit claims.

The above list is not all inclusive or mutually exclusive, but shows the problem of selecting safety benefit measures without overlapping.

Difficulties encountered in safety-related benefit-assessment include the fact that large, complex projects (i.e., a complex aircraft weapon system development) may not offer benefits to the same people who are at risk. Other difficulties include: 1) how to assess the difference between a low probability incident having catastrophic consequences i.e., loss of life, and a high probability incident having marginal consequences, i.e., minor injury and 2) determining the probability of multiple fatality/mishaps/ injuries versus a single-fatality/mishap/injury event.

Then there is the problem of not only measuring but determining what the "avoided cost " benefits are. Avoided costs may be strictly economic (i.e., the losses of net

output of goods and services due to property damage, personal injury and death [Ref. 25:p. 107]), or abstract (i.e., avoided pain from injury, increased operational effectiveness). Direct economic benefits could include avoided engineering aircraft change proposals, avoided aircraft mishap costs, avoided pilot losses, and indirect economic benefits would include avoided loss of output to the economy (foregone earnings) resulting from death or disability.

In conjunction with these economic benefits would be economic costs due to lower attrition rates resulting in increased pilot retention rates and numbers of aircraft to maintain.

Since economic benefits/costs (direct and indirect) are relatively more concrete compared to the losses received by the victims, i.e., in this case the military services or their families. There is a tendency to use economic costs in making management decisions. A correct interpretation of economic costs is that they are the lower bound costs society would spend to prevent accidents.

Noneconomic losses aren't usually taken into consideration but probably should be, in many cases. These losses have two parts: 1) pain, fear, and suffering of the victims involved, and 2) loss of consumption on the part of the victim and family. There is little dispute that these losses should be added to the economic losses described

above, the problem is difficult to see how to quantify them in a way that will fit into a social accounting system necessary for evaluating different projects. [Ref. 25:p. 107]

Benefit-cost analysis studies are now being performed much more routinely as an integral part of safety studies, but there is no agreed-upon methodology for identifying or quantifying benefits. More over, the use of the results of such benefit analyses varies widely. The level of risk which is deemed acceptable is either not known quantitatively or varies depending on the decision maker or regulatory body. Hence, the overall reduction in risk which must or should be achieved in fairly arbitrary. [Ref. 24:p. 9]

A first step in estimating the benefits of a safety regulation is to estimate the reduction or avoidance of injuries, illnesses, and fatalities that the standard will produce. Safety outcomes may be estimated from data on injury rates, aircraft mishaps, and their causes with judgmental consideration given to the effect the safety regulation has in avoiding or reducing injuries, mishaps, and their causes.

Other problems associated with a benefit-cost safety analysis include difficulties in identifying the full range of not only benefits but costs (including those accruing to other than the sponsor and intended beneficiaries,

differentiating benefits from costs, choosing an appropriate discount rate (if required) for comparing costs and benefits overtime, selecting the appropriate criterion for comparing benefits (i.e., net present value or benefit-cost difference); and handling multi-attribute outcomes. [Ref. 24:pp. 11-12]

Even though difficult problems exist in performing a safety assessment, economists and others feel the concept provides a useful framework for thinking about a proposed action or comparing alternatives even if its not possible to do it in a wholly quantifiable way. However, without better resolution of these methodological problems, decision makers or proponents of the action may have a tendency to assign unduly high values to those benefits which are important but hard to measure, while opponents may tend to over emphasize the fact that the benefits which are easiest to quantify and value are relatively small. [Ref. 24:p. 12]

V. METHODOLOGY

The first section of this chapter provides an overview of System Engineering and System Engineering Specialties. System Engineering and management techniques help to ensure that cost, schedule, and technical performance (CSTP) objectives are met when developing a weapon system. System safety is identified as a system engineering specialty and is considered a prerequisite to obtaining CSTP objectives.

The second section provides a standardized approach to use when performing a system engineering cost-effectiveness evaluation. The approach has 10 steps. Each step is reviewed briefly.

The third section defines what "system effectiveness" is and provides an overview of a multi-attribute model which may be used to evaluate a system's effectiveness. System safety isn't considered a major program objective in the multi-attribute model--but could be if it was identified as such. In conclusion, system effectiveness models could be considered as one possible way of determining the cost-effectiveness of system safety.

A. SYSTEM ENGINEERING/ENGINEERING SPECIALTIES

> There has been an emerging awareness of the need for and the importance of total system design. System engineering is fundamentally concerned with deriving a coherent total system design to achieve stated objectives. No two systems are ever alike in their developmental requirements.

> However, there is a uniform identifiable process for logically arriving at system decisions regardless of system purpose, size, and complexity.
>
> Systems Engineering Managerial Procedures
> AFSCM 375-5

The past several decades have seen the rise of large, highly interactive systems that are on the forward edge of technology. This is especially true in DOD where their motivation is the basic security of the Nation. These technical systems have a natural process of evolution, or life cycle, in which actions taken (or not taken) in the very early stages can mean the difference between success and failure. [Ref. 26:p. 1-i]

The purpose of System Engineering is to prevent these failures through a unified approach that completely defines all requirements on the system and establishes a system configuration which is proven early-on to be capable of meeting certain requirements. System engineering is often referred to as a "frontend" process. That is, the majority of System Engineering tasks are completed in the initial phase of a program, when about 5 percent of a program's funding is expended. This initial effort results in defining the configuration and size of the system and its logistic support. The resulting program commitment of funds typically represents 90 percent of program life cycle costs. Accuracy and completeness of the early System Engineering effort is therefore essential in maintaining a program within budget constraints. [Ref. 26:p. 1-i]

While the definitions of system and system engineering depend somewhat on the application and are nearly as numerous as the practioners. A statement made concerning system engineering several years ago:

> . . . for more than a decade, engineers and administrators have witnessed the emergence of a broadening approach to the problem of designing equipment. This phenomenon has been poorly understood and loosely described. It has been called system design, system analysis, and often the systems approach. [Ref. 22:p. 27]

In the ensuing years since this statement was made, there have been numerous efforts to describe system engineering, both in an abstract sense, and as a methodological disclipine. A definition applicable to DOD programs is:

> System Engineering is the application of scientific and engineering efforts to (a) transform an operational need into a description of system performance parameters and a system configuration through the use of an interactive process of definition, synthesis, analysis, design, test, evaluation; (b) integrate related technical parameters and ensure compatibility of all physical, functional, and program interfaces in a manner that optimizes the total system definition and design, (c) integrate reliability, maintainability, safety, survivability, human, and such factors into the total engineering effort to meet cost, schedule, and technical performance objectives. [Ref. 26:p. 1-1]

An examination of the preceding definition of system engineering reveals the following key words and their implications:

WORD	IMPLICATION
1. Desired ends	Need
2. Resources	Input
3. Systems or devices	Outputs

4.	Process	Transformation (synthesis)
5.	Optimally convewrted	Criterion of worth, constraints, analysis, evaluation, optimization,
6.	Decision Making	Choice (evaluation)
7.	Iteractive	Feedback (optimization)

Essentially system engineering is a feedback control system for transforming a set of inputs in an optimal manner within certain allowable constraints to meet stated needs in accordance with a defined measure of worth. [Ref. 22:p. 28]

Over the past several decades, as complex systems have evolved and matured, the problems encountered in the "management" of these systems have caused DOD to develop a systematic engineering management process that directs periodic review and control of a program throughout its acquisition and operational life.

In 1976, the Office of Management and Budget (OMB) Circular A-109 was published. The philosophy behind OMB Circular A-109 is for the Government to become a more reliable customer by standardizing its acquisition policies throughout the Government in order to avoid major contract delays and cancellations, and to promote an unbiased concept definition. It requires that the Government operating agency establish and justify a valid requirement for capability, which must be approved by the executive agency head (Secretary of Defense, NASA Agency, etc.) before

involving industry in the system acquisition process. The approval of this needed capability also established the priority and theoretically the availability of resources to fulfill the need.

In March 1982, DODINST 5000.1, Major Systems Acquisition, was revised to reflect the following acquisition management principles:

- Ensure effective design and price competition
- Improve system readiness and subtainability
- Increase the stability in acquisition programs through effective long-range planning, use of evolutionary alternatives instead of solutions at the frontier of technology, realistic budgeting and funding programs for the total life cycle, and planning to achieve economical production rates
- Delegate authority to the lowest levels of the service that can provide a comprehensive review of the program
- Achieve a cost-effective balance between acquisition costs, ownership costs, and system effectiveness in terms of the missions to be performed.

In conjunction with DOD 5000.1, System Engineering identifies and defines the functional characteristics of system hardware, software, facilities, and personnel through an interactive process of analysis and design, with the objective of satisfying an operational mission need in the most cost effective manner. The System Engineering process analyzes mission requirements and translates them into design requirements at succeeding lower levels to insure operational satisfaction. Control of the evolving development process is maintained by System Engineering

through a continuing series of reviews and audits of technical documentation produced by supporting organizations. [Ref. 26:p. 1-11]

The output of System Engineering is documentation. This is the means by which it controls the evolutionary development of the system. During the Demonstration/Validation phase, System Engineering prepares a number of plans that define how the Full Scale Development phase will be conducted and cover primarily the engineering speciality areas. These plans are usually submitted with the FSD proposal in draft form. Final plans are a part of the FSD phase Contractor Data Requiremetns List, submitted usually within several months after contract go-ahead, except for those areas closely associated with deployment and operations. They are used by Government organizations to ensure compliance with standard policies and procedures in these areas, and by contractor personnel to develop detailed schedules and to plan allocation of resources. Specifications prepared by System Engineering form the basis for the design and development effort. The top level specification (system, segment, or configuration item) is incorporated in the FSD Statement of Work and becomes the Government's document. Requirements are flowed down and allocated to lower level specifications, which designers and subcontractors translate into hardware and software. As the system development progresses, System Engineering documents status

in the form of design review packages, test performance measurement reports, analysis and simulation reports, and other documentation, which provides the Government with a continuing assessment of the capability to meet performance requirements. [Ref. 26:p. 1-12]

This documentation may include:

- System Engineering Management Plan
- System, segment, prime item, and computer program configuration items specifications
- Interface Control Documents
- Risk Analysis Management Plan
- Survivability/Hardness Plan
- System Design Review data packages
- Mission analysis reports
- Functional flow, functional block, and functional interface diagrams
- Reliability Plan
- Maintainability Plan
- Safety/Hazard Analysis Plan
- Human Engineering Plan
- Integrated Logistics Support Plan
- Electromagnetic (EM) Compatibility and EM Interference Control Plan
- Parts, Materials, and Processes Control Plan
- System Test Plan
- Mission Support Plan
- Audit reports.

Engineering specialities are integrated into the development through the System Engineering process. Engineering specialties are those disciplines which support the design process by applying knowledge from a specific area to ensure system operability in its operational environment. Engineering Specialties include reliability, maintainability, human engineering, transportability, system safety, electromagnetic compatibility, parts/materials and processes and other specialist areas involved in development of a general class (ships, aircraft, tanks) of a system. Specialty engineers draw upon an extensive background of data extracted from past and current programs to develop standards, guidelines, and checklists to support and evaluate the development of new designs. [Ref. 26:p. 15-1]

The role of the specialist under System Engineering is to define requirements for design and verification, to audit the resulting design for compliance, and to plan all activities related to their functions.

B. 10 STEP SYSTEM ENGINEERING COST-EFFECTIVENESS EVALUATION APPROACH

The objective of system engineering is to maximize some parameter of a system's worth in terms of effectiveness or performance by means of a design. A system's worth is basically a function of the differences between its benefits and its costs. However, absolute differences of themselves

provide no true criterion of worth. They must be related in some way to a scale of particular value.

For example, a dollar profit is usually evaluated as a percentage gain on an amount invested. A gain in speed is meaningful as a percentage increase over some reference value of speed. A 5-mph increase might be considerable for a 50-mph tractor but inconsequential for a jet airplane. [Ref. 22:p. 5]

A particular engineering activity or decision may result in a gain in benefit over cost for one component of the value at the expense of a loss for some other. Thus a trade-off situation exists. In order to conclude the worth of the one value in terms of the other, there must be a value scale for relating them. [Ref. 22:p. 5]

In the most general sense then the objective is to maximize system worth or "utility."[1] Thus:

$$\text{Maximize} \qquad \mu = f(x_1, x_2, x_3, \ldots, x_c \ldots x)$$

where $\{x_i\}$ are the value variables. Some are positive (benefits); others are negative (costs).

It should be emphasized that this is not a restricted meaning of cost-effectiveness. When the term "cost-effectiveness" is popularly used it is often implied that costs

---

[1]Utility means usefulness, the satisfying of a need. A decision or an outcome has high utility when it satisfies a need as well as it can with the available resources.

are dollars and effectiveness is system effectiveness in an operational sense. System worth may be conveniently subdivided into three major components:

1. System performance (performance effectiveness).
2. Time (time effectiveness).
3. Money (monetary effectiveness) as a common measure of resources.

Practice may often be restricted to the conditional requirement of the following:

1. Given a required performance and schedule, minimize dollar cost as weighted by time.
2. Given a time weighted cost, maximize performance.

These are extremes; the optimum system that maximized system worth will usually fall between them.

A system is time-limited. It takes time to realize the need. It takes time to develop a system to satisfy it. Finally, the system operates to satisfy it. The entire time span or system life cycle must be considered in relation to the system effectiveness. Time is one of the costs. In actuality, the realization of the time relationship leads automatically to the need for considering cost over the system life cycle. Time may be valued in money. The values are threefold.

1. The worth of time ot make decisions (flexibility);
2. The worth of time for schedule of output. (This may be a value of time remaining on a schedule, given an established schedule);
3. The worth of time for waiting for a promised future system value to materialize.

System Engineering is concerned with the design of a new system which is expected to produce a desired result over time. Thus, system engineering techniques must predict the future, but the future is uncertain. This uncertainty must not only be accepted but must also be taken into account in the design. Therefore, an appreciation for the basic elements of probability must exist.

All decision problems contain the following elements.

1. A set of alternative actions the decision maker might select;
2. A set of conditions which reflect the possible environment in which the decision is to be made, often called states of nature or states of the world;
3. A set of outcomes which may result, depending upon which action is chosen and which of the environmental conditions do in fact exist at the time the action is taken;
4. A value or utility to the decision maker resulting from the outcome;
5. Some assessment of the likelihood or probability of each of the states of nature being the true one when the action is taken.

In evaluating the cost-effectiveness of advanced systems the following prerequisites must be recognized.

1. Common goals, purpose, or mission of the systems must be identified and at least theoretically attainable.
2. Alternative means of meeting the goals must exist.
3. Constraints for bounding the problem must be discernible.

Without common goals, the evaluation is meaningless, for example, comparison of an airplane with a computer would be nonsensical. If there is only one feasible system for

achieving the goal, there is no latitude for comparative evaluation. By recognizing and specifying constraints, one bounds the evaluation and the preferred systems within these constraints can then be identified. [Ref. 27:p. 114]

It should be recognized that the preferred systems are such for only the specified goals and constraints. By subtle alteration of the goals and constraints, different systems frequently can be made to look best.

A serious problem in cost-effectiveness terminology frequently arises when reference is made to the requirements associated with the goals of missions to be fulfilled by the systems. To give the goals tangible meaning, their requirements must be specified. These requiremetns will be referred to below as "mission requirements."

Mission requirements are those attributes that must be met in evaluation of systems to fulfill their goals. Unfortunately, the term "system requirements" is frequently used for these attributes, which results in semantic ambiguity because it is never clear whether the requirements are imposed on or by the system. Hence, "mission requirements" will refer to those elements of the goals that must be met by the system capabilities. Evaluation criteria constitute measures by which the suitability of the candidate systems to fulfill the desired goals is judged or evaluated. The aim of the cost-effectiveness evaluation is to identify the system whose capabilities meet the mission

requirements in the most advantageous manner. [Ref. 27:p. 115]

The following 10 steps constitute the standardized approach to conducting a cost-effectiveness evaluation on advanced systems. Although the steps are presented in the order in which they would generally be performed, changes in the sequence are sometimes desirable, depending on the idiosyncrasies of the evaluation.

1. Define the desired goals, objectives, missions, or purposes that the systems are to meet or fulfill.
2. Identify the mission requirements essential for the attainment of the desired goals.
3. Develop alternative system concepts for accomplishing the missions.
4. Establish system evaluation criteria (measures) that relate system capabilities to the mission requirements.
5. Select a fixed-cost or fixed-effectiveness approach.
6. Determine capabilities of the alternative systems in terms of criteria evaluation.
7. Generate systems-versus-criteria array.
8. Analyze merits of alternative systems.
9. Perform sensitivity analysis.
10. Document the rationale, assumptions, and analyses underlying the previous nine steps. [Ref. 27:p. 116]

1. Step 1: Define the Desired Goals

A key characteristic of those analyses that fall within the term "cost-effectiveness evaluations" is that the goal or goals can be met by a single system (or program). The purpose of the cost-effectiveness evaluation is to

identify the "best" system for attaining the specified goals. For example, a governmental agency might conduct an evaluation to determine the most desirable smog control device for automobiles. Similarly, the agency might also want to evaluate the comparative merits of expending funds on air pollution versus stream pollution. However, in this latter type of decision, a new element has been introduced--both of the goals are desirable and they cannot be fulfilled by a single system. This charactgeristic transfers the analysis and evaluation associated with arrivnig at the "best" decision, from cost-effectiveness per se to resoruce allocation. What is really desired is not the best system for meeting the goals but rather the best allocation of available resoruces among the alternative opportunities. Conducting a cost-effectiveness evaluation to determine the best smog control device for automobiles may be a perfectly valid and legitimate application of that technique. However, if the decision required is really how best to expend funds for the elimination or reduction of air pollution (which cannot be accomplished by any one "system"), the solution falls into the domain of resource allocation. The resource allocation decision should incorporate assessment of such actions as subsidizing the manufacture of electric-powered automobiles by elimination of the excise tax, the policing of soruces of pollution (refineries, primary metals industries, and so on), in

addition to any other controllable activities that have an impact on the problem. [Ref. 27:p. 116]

To perform a meaningful evaluation of alternative systems it is necessary first to establish the specific goals or missions that the systems are to fulfill. Without such an identification of goals there is no framework for structuring the subsequent evaluations. Usually the goals are identified at least in a general manner by the requesters of the evaluation. The level of generality with which the goals are specified and the inherent optimism implicit in the goals constitute two problem areas in goal definition. If goals are specified in too general terms (motherhood and country; i.e., eliminating poverty, destroying the enemy) the constraints established by the analyst for bounding the evaluation are the product of his imagination and interpretation of the goals rather than the product of the goals per se. On the other hand, care must be taken not to make mission goals too specific or they limit the scope of possible candidate systems by implicitly defining system concepts rather than just the desired goals.

A potential danger always exists in that the goal setter may specify a goal that is unattainable by means of current (or reasonably advanced) technology. Most new systems contain a significant element of research and development. The problem is how to make the fine

distinction between attainable and unattainable advances in technology.

Care must be exercised not to identify the goals in such a manner as to bias the evaluation by including requirements of such a specific nature that they exclude from consideration potential candidate systems. The point here is that, while specific goals need to be identified, care should be taken to avoid including extraneous goals or system-biasing methods of attaining the goals.

2. Step 2: Identify Mission Requirements

One of the basic purposes of defining unambiguously the specific goals or mission is the facilitation of the identification of mission requirements whose fulfillment is essential to the attainment of the goals or missions. The mission requirements should be identified as parametrically as possible so as to reduce the possibility of biasing the evaluation. For example, in a comparison of military transportation systems, one system may be capable of delivering many men but relatively little supporting materiel, while another system may be capable of delivering large quantities of materiel but relatively few men. By specifying a number of men and/or materiel as a fixed requirement, one may unnecessarily bias the subsequent evaluation. This bias could possibly be eliminated by the establishment of a relationship that converts man and materiel into fighting man-days. The expression of the

mission requirements in this manner could portray in a more meaningful manner what is really desired. [Ref. 27:p. 119]

The identification of mission requirements that are pertinent derivatives of the goals to be fulfilled usually requires judgment sharpened by experience. Errors of commission are just as deceiving as errors of omission, in that if mission characteristics that are not necessarily essential to the successful fulfillment of the mission are identified as requirements, they can strongly prejudice the subsequent evaluation. Instances have occurred in which so many mission requirements were identified in such a specific manner that (unknowingly) it was physically impossible to accomplish the mission with any system. The "let's be safe and include everything" approach is not a substitute for judgment and experience. On the other hand, it is obvious that the omission of significant mission requirements could readily result in an invalid conclusion. Somewhere between the too-many mission requirements and the too-few mission requirements is the elusive "just right." [Ref. 27:p. 119]

3. Step 3: Develop Alternative Systems

Once the mission requirements have been identified, the next step is to develop alternative system concepts that can meet (or exceed) them. If only one system can be conceived, any further implementation of a cost-effectiveness evaluation for purposes of system selection is futile. To conduct a meaningful evaluation, at least two distinct

candidate systems must be conceived. The alternative systems should be dissimilar if the evaluation is to be conducted on the system level. For example, if the key difference between candidate systems is basically one major subsystem, the evaluation should be reduced in scope and focused on the subystem (if the effects of all other system characteristics are common to both systems and thus cancel out). [Ref. 27:p. 120]

In attempting to implement this step the practitioner quickly encounters a serious problem: the depth of detail associated with system definition. Since the purpose of the evaluation is usually to aid in deciding which of alternative systems should be developed, specific details of the systems are generally lacking. Too little system definition usually results in a large variance in system effectiveness and cost. On the other hand, to require that the candidate systems be designed in detail before being evaluated would defeat the basic purpose and value of cost-effectiveness and negate the major benefits accruing from the cost-effectiveness evaluation. A basic guide to the appropriate depth of detail in system synthesis is that it be conducted to that depth that lends confidence to the ansers. [Ref. 27:p. 121]

4. Step 4: Establish System Evaluation Criteria

Numerous papers discussing cost-effectiveness have been written during the past several years. Unfortunately,

many of them create only confusion rather than clarification by presenting discussion of cost and effectiveness within different, and sometimes unique, semantic frameworks. General discussions of the philosophical aspects of cost-effectiveness are usually conducted on a high level of abstraction. However, meaningful evaluations cannot be conducted on these lofty levels because of the very lack of detailed specificity inherent in the general terms that makes their use so attractive for philosophical discussion. [Ref. 27:p. 123] Four indenture levels of terminology associated with cost-effectiveness evaluations are shown in Figure 5-1.

Under Program cost, the third indenture level (1, 2, 3, 4) could be divided readily into at least two additional levels. The semantic problems generally do not stem from the cost side of the evaluation, but rather from the effectiveness side. Under Effectiveness, A through G indicate typical terms that are often used to imply the concept of effectiveness. Utility tends to be favored by economists. Productivity tends to be favored by persons who are inclined to focus attention on the results to be derived from the systems being evaluated. Worth tends to be favored by engineers. Merit or figure-of-merit is a carry-over from operations research, where one of the key steps in solving an operational problem is to identify an appropriate figure-of-merit. Where the solutions (systems) need to satisfy a

Program Cost

A. System cost to accomplish specified mission(s)

   1. RDT&E
   2. Procurement
   3. Operating
   4. Other

B. Funding rate

C. Resources required

Effectiveness

A. Utility

B. Productivity

C. Worth

D. Merit

E. Benefit

F. Gain

G. Value received

   1. Performance
   2. Lethality
   3. Economy
   4. Safety
   5. Mobility
   6. Accuracy
   7. Maneuverability
   8. Availability
   9. Flexibility
  10. Prestige
  11. Damage to target
  12. Maintainability
  13. Reliability
  14. Probability of mission success
  15. Evolutionary development
  16. Growth potential
  17. Information received
  18. Security
  19. Survivability
  20. Vulnerability
  21. Penetrability
  22. Repairability
  23. Dependability
  24. Capability
  25. Abortability
  26. Technical confidence
  27. Scientific information yield
  28. Mission versatility
  29. Value of targets destroyed
  30. Spillover effects
  31. Technical desirability

Figure 5.1 A Standardized Approach to Cost-Effectiveness Evaluations

a. Weight capability
b. Reaction time
c. Reliability
d. Range
e. Speed
f. CEP
g. Deg/sec turn
h. Init. oper. cap.
i. S/lb
j. Productive scientific man-hr
k. Prob. of target destruction
l. Ton-miles/hr
m. U.S. lives lost
n. Cost to enemey to counter
o. Service life
p. Power
q. Energy
r. Expected profit

Figure 5.1 (Continued)

number of criteria, as is often the case in cost-effectiveness evaluations, thebasing of the evaluation on a sole figure-of-merit is generally inadequate. [Ref. 27:p. 123]

Benefit is favored by the Bureau of the Budget. Gain is favored by some economists while value received is one other way of viewing effectiveness.

The third indenture level (1 through 31) contains terms that possess greater specificity than the second indenture level (A through G). However, this specificit is deceptive.

Reliability is considerd to be a very specific, quantitative attribute. However, in evaluation of systems, all system attributes must undergo a penetrating analysis to ascertain exactly what is meant, implied, or measured by that attribute. Reliability is often defined as "the probability that a device will perform without failure of a specific function under given conditions for a given period of time." To use this term to describe quantitatively some attribute of a complex weapon system or space system (as is often done) raises serious problems of interpretation. Precisely what is jmeant by asserting that a manned spacecraft system has 0.93 reliability? Generally, it is interpreted to mean that 93 times out of 100 the system will perform as planned. Does it mean that no bulb will burn out, no valve will stock, no toggle switch will fail, and so on, on 93 of the 100 missions? If it means that subsystems

essential to the performance of the mission will not fail on 93 of the 100 missions, how is the determination of what constitutes an "essential subsystem" made? Many subsystems are highly desirable and hence are incorporated into the spacecraft, but does this make them essential? For example, if the food-warming system failed, should that mission then be counted as one of the 7 out of 100 anticipated failures? The point being made is that reliability figures, when applied to complex, manned systems, rather than conveying a hard, quantitative measure of a very specific attribute, upon close analysis are found to be generally meaningless. [Ref. 27:p. 124]

Safety is one of the most difficult criteria to identify and evaluate. Western society tends to place an almost infinite value on human life. Of course, space missions would never be undertaken if some risk (in the nonmathematical sense) were not acceptable. Past attempts to relate this risk (or value of human life) to dollars have not proven successful. Yet even a cursory analysis can yield interesting conclusions: almost every individual considers something more dear than life. Newspapers often make mention of individual sacrifices that likewise illustrate the rational acceptance of a substantial risk of life. Fortunately, the need for physical demonstrations of this willingness to risk one's life are relatively rare. However, the high cost of rescue on space missions, for

example, necessitates a critical examination of the attributes and possible alternative views of safety. It is recognized that the risk of death accompanies many accepted human activities and that these risks are realized and accepted. (For example, the risk associated with air travel is accepted for the greater convenience of air travel.) It might be productive to consider safety in terms of risk and reward. For example, rather than establish a very high degree of safety (like 0.9999) as a space mission constraint, or require a space rescue capability with its associated high cost and uncertainty of success (that is, can rescue be accomplished in time?) would not a preferable alternative be to specify a mission crew safety of 0.99, with the understanding that in lieu of greater safety or development of a space rescue capability, the astronauts would receive a $100,000 (or even a $1,000,000) bonud, or some figure commensurate with the risks involved for undertaking the mission. In many professions today, the pay scale is commensurate with the training, skill, and risk involved (deep-sea divers, test pilots, and so on). By developing an acceptable variation to what could otherwise be a constraint, systems that would otherwise not be feasible (for example, if greater safety were required) can become candidates for consideration. Penetrating analyses are frequently required to arrive at an understanding of the essential concepts inherent in terms such as safety,

prestige, technical desirability, and so on. [Ref. 27:p. 125]

The previous comments are important for analyzing the cost-effectiveness of system safety. For system safety, the question is: "How much system safety should be required in the development of advanced weapon systems (i.e., naval aircraft)?"

Although they are not uniquely expressible in a quantitative manner, some of the third-level criteria are significant to most evaluations. They should not be ignored or falsely quantified. Instead, the candidate systems should be verbally evaluated in terms of these criteria by discussion of the relative capabilities of the systems to satisfy those criteria that are pertinent. [Ref. 27:p. 125]

The fourth indenture level (a, b, c, d, and so on) lists typical quantifiable criteria used for evaluating alternative systems. In almost all evaluations, some significant criteria are quantifiable. Evaluations should always be based on and expressed in terms of the most specific (not necessarily detailed) criteria that are meaningful. [Ref. 27:p. 125]

The selection of appropriate and adequate criteria is based on judgment augmented by experience. The omission of significant criteria could readily invalidate the results of an evaluation. Thus, rather than simplifying the evaluation, the inclusion of criteria with low levels of

pertinence unnecessarily complicates the evaluation and its subsequent implementation. [Ref. 27:p. 126]

A simple test of the adequacy or completeness of criteria for evaluation is to question whether one system could excel in most of the criteria generated and still not be deemed "best." If the answer is affirmative, important criteria are missing. By their very nature, military systems generally require consideration of aspects of vulnerability, reaction time, and detectability in their evaluation. Considerable insight into the subtleties of the goals and mission requirements is usually necessary for the generation of other meaningful evaluation criteria.

5. Step 5: Select Fixed Cost or Fixed Effectiveness Approach

The choice between fixed cost and fixed effectiveness is necessary in virtually all cost-effectiveness analyses and is, in general, a nontrivial decision. In the fixed-cost approach, the basis for selection between alternatives is the amount of effectiveness obtained for a given expenditure of resources. On the other hand, in the fixed-effectiveness approach, the selection criterion is the amount of cost incurred or resources required to obtain a given level of effectiveness. If there is only one well-defined measure of cost to which the resources required may be directly related and only one pertinent criterion of effectiveness, such as targets destroyed, orbital payload delivered, and so on, there will not be any significant

difference between the results obtained by these approaches, since the fixed-cost and fixed-effectiveness approaches will merely be mirror images of each other. In such cases, the choice of approach will not affect the results of the analysis within given economic and effectiveness boundary conditions. [Ref. 27:p. 127]

a. Fixed-Cost Approach

A basic step in the fixed-cost approach is the identification of the candidate systems that are competitive for the given resources. Then the number of units of each system that can be developed, procured, and operationally implemented with the fixed resources is determined. Finally, the degree to which each alternative satisfies the goals or mission requirements is estimated, and that system which fulfills the goals to the greatest extent is judged to be best. [Ref. 27:p. 128]

b. Fixed-Effectiveness Approach

In the fixed-effectiveness approach, the procedure discussed above is reversed, with the desired level of effectiveness specified by way of the mission requirements. The alternative systems taht can fulfill these requirements are evaluated competitively with the evaluation being based on the total penalties or costs incurred by each alternative. [Ref. 27:p. 128]

6. Step 6: Determine Capabilities of Alternative Systems

Once the appropriate criteria have been identified, the next step is to express the abilities of the candidate system in terms of the criteria, quantitatively if possible, qualitatively if not. [Ref. 27:p. 129]

7. Step 7: Generate System versus Criteria Array

Two different techniques of conducting cost-effectiveness evaluations within the fixed-cost or fixed-effectiveness approaches are often encountered: (a) the model approach, and (b) the tabular display approach. The model approach, in which a cost or effectiveness model is generated, is usually used when the basic differences between the candidate systems are relatively minor, so as to permit the valid expression of their essential differences by a single parameter. [Ref. 27:p. 129]

a. Model Approach

The use of mathematical effectiveness models is warranted only when the systems being evaluated are basically so similar that those evaluation criteria that cannot be readily qualified or interrelated cancel out, thsu leaving only quantifiable and commensurable criteria. Mathematical cost models are much more frequently encountered. While exhibiting significant advantages for specific applications, they also possess substantial limitations. The key advantage of the use of mathematical cost

models is the rapidity with which a number of systems can be costed. [Ref. 27:p. 129]

b. Tabular Display Approach

The tabular display approach is used when the systems are being evaluated on the basis of either quantifiable criteria that are incommensurable, or by both quantifiable and unquantifiable criteria. In this approach the criteria underlying the evaluation are identified at the tops of columns and arranged in decreasing importance of criteria, from left to right (see Figure 5.2). The alternative systems are then listed vertically, with the alternative that meets the firt (most significant) criterion to the greatest extent listed first, and so on. This approach is particularly useful when many alternative systems are being evaluated because it can be used to eliminate the less likely candidates and focus attention on the two or three major contenders. The ultimate selection is then generally based on a judicial evaluation of system capabilities and mission requirements. [Ref. 27:p. 133]

8. Step 8: Analyze Merits of Alternative Systems

Once the candidate systems are arranged in order of their capability of satisfying the most important criterion or criteria, it is generally possible to eliminate the poorer candidates and focus attention on the top three or four candidates. If the effectiveness criteria and cost considerations for the top contender are consistently

System	Cost Constraints (Verbal)								Mission Requirements: (Verbal)					
	Dollar Cost						Scarce Manpower Required	Scarce Material Required	Effectiveness Criteria					
	Total $	RDT and E		Procurement		Operational								
		Years	$	Numbers	Years	$	Years	$						
1									AAA	BBB	CCC	DDD	EEE	Etc.
2														
3														
4														
.														
.														
.														
N														

Source: [Ref. 27:p. 132]

Figure 5.2 Typical Tabular Array for Cost-Effectiveness Evaluation

superior to the respective values for the other candidates, that system is dominant and the selection is obvious. If the criteria values for the top two contenders are virtually identical, and no significant difference in costs exists, the appropriate answer may be that, based on current knowledge and assumptions made, there is no significant difference between the top two contenders, in which case the adoption of parallel study or development efforts may be indicated in order to identify the superior system. If the system costs differ significantly and preferences shift among the criteria, which also differ significantly, the selection will need to be made on the basis of value judgments. [Ref. 27:p. 135]

The merit of this approach is that it clearly presents the basis on which the selection was made. The selection may be vetoed by higher levels of decision-makers who may incorporate high-level criteria into their evaluation, but the basis on which the initial system selection was made is apparent.

An argument sometimes presented against any approach based largely on the verbal presentations of value judgments is that it is highly subjective. In reality, value judgments usually portray the realities of the situation much more accurately than does the use of numerical values alone. The use of numbers requires the expression of multi-faceted relationships by discrete integers; for example, the

payload capability of candidate systems may be 2000, 3000, and 4000 pounds, respectively. If the minimum acceptable payload is 2000 pounds, the normalized ratios would be 1, 1.5, and 2. (How tempting to combine with other normalized criteria!) But what is the significance of a capability to carry 1000 or 2000 pounds more than that required? The importance of this excess payload capability to the attainment of the mission goals may be substantial or it may be insignificant. If it is recognized that the function of the analyst is to communicate to the decision-maker the resutls of his knowledge, experience, and judgment with respect to the particular evaluation at hand, the sole use of numbers (either the original number or ratios) for even quantifiable criteria, much less for unquantifiable criteria, is a coldly sterile approach. In reality it is almost insulting because of the implicit assumption of "rightness" inherent in the use of numbers. By the use of verbal portrayal (in addition to the use of numerical values for quantifiable criteria), the multifaceted interrelationships between systems and criteria, which are multidimensional impressions based on the knowledge, experience, and judgment of the analyst, can be more readily conveyed to the decision-maker. The probability of successfully communicating the impact of the real-world multidimensional interrelationships between systems, criteria, and goals is much higher by the verbal expression of value judgments and the underlying rationale than by the

attempted expression of these facts and judgments through the sole use of numerical values. The tabular approach permits the orderly presentation of systems capability data so that their impact on the evaluation can be readily discerned and discussed along with the significant interrelationships. Thus, conclusions can be reached by visible, traceable means. [Ref. 27:p. 136]

9. Step 9: Perform Sensitivity Analysis

In many instances the outcome of a cost-effectiveness analysis is very sensitive to the assumptions made. In such cases the conclusions reached may be unknowingly yet significantly biased by the innocuous assumptions essential to the analysis; for example, the assumptions of a linear relationship between two parameters may, in fact, be more accurately depicted by an exponetial relationship (such as weight versus reliability, cost versus CEP, unit procurement cost versus total quantity procured), or an exponential-appearing relationship may, in reality, flatten out to a Gompertzian curve. To be assured that the results are not dependent upon such biases, it is essential that a sensitivity analysis be performed. In this analysis, the assumptions that were made initially are modified, different values of the variables are assumed, and then the impact of the variations on the resultant evaluation is determined. If the results of the analysis are shown to be very sensitive to certain assumptions, either sound justification

for the use of the assumed values must be developed or the sensitivity of the conclusions to the assumed values should be indicated and emphasized. [Ref. 27:p. 138]

10. Step 10: Document Bases of Previous Nine Steps

A cost-effectiveness evaluation is incomplete without a detailed documentation of its purpose and assumptions, the methodology employed, and the conclusions reached. Without such documentation, a clear understanding of the significance and limitations of the conclusion(s) is unavailable. No prudent decision-maker would base a major decision on blind trust in the analyst and his conclusions. There is no substitute for a clear understanding of the evaluation to lend credibility (not necessarily agreement) to the results. Particular emphasis should be placed on lucide documentation of the following.

1. Specific goals to be attained.
2. Essential requirements of those goals, along with associated assumptions.
3. System capabilities and associated assumptions.
4. System costs and associated assumptions (learning curves, times, quantities, and so on).
5. System evaluation and associated assumptions (scenarios, criteria, and so on).
6. Conclusions--their limitations and sensitivity.

The use of highly esoteric mathematics should be discouraged. By expending some effort, imagination, and thought, the analyst can usually suitably portray complex mathematical relationship in simplified (perhaps graphic)

form. It should be recognized that no judicious manager or administrator can be expected to endorse a conclusion or recommendation whose rationale and derivation he cannot fully understand. It is the responsibility of the analyst to present the documentation in an appropriate manner. It is deemed preferable to use simple, understandable techniques so as to arrive at an acceptable near-optimum recommendation that is implemented rather than to use esoteric techniques to define a precise optimum recommendation that runs the risk of being relegated to dust-gathering because the responsible decision-maker(s) can neither follow nor comprehend the rationale underlying the techniques employed. [Ref. 27:p. 139]

In summary, the following conclusions are made regarding this cost-effective analysis decision-making process:

1. The standardized approach presented herein is not the only valid way to conduct a cost-effectiveness evaluation, but it has been applied successfully and is readily understandable.

2. Use of the approach described is not a guarantee to a successful evaluation, in that judgment and experience are still required. However, the specific areas that are very sensitive to experience and perceptive judgment are identified, so that particular attention may be focused on them.

3. Use of this approach will make possible the focusing of disagreement on very specific points. Heretofore, the lack of acceptance of the results of an evaluation has generally resulted in a blanket indictment of cost-effectiveness per se. By ready identification of specific points, additional research done, or more extensive sensitivity analyses performed, so as to resolve disagreements, will thus make possible the

achievement of a rational consensus--which, after all, is one of the practical products of cost effectiveness evaluations.

4. If advanced mathematical techniques provide insight or even reveal uniquely the most desirable system, the analyst should place major emphasis on simplifying the mathematical complexity of the analysis maker. Pride in the mathematical complexity of the analysis should be exchanged for pride in the clarity, validity, and comprehensibility of the evaluation. Admittedly, not all complex problems can be solved by simple techniques, but disallusion to the mathematical sophistication of the analytical process does not lend credence to the answers obtained.

5. This approach is admittedly an initial step at formalizing the methodology for conducting cost-effectiveness evaluations. It does provide a much-needed frame of reference for the diverse elements that can be introduced into an evaluation. The standardized approach presented constitutes a road map to the conduct of cost-effectiveness evaluations. [Ref. 27:p. 149]

C. SYSTEM EFFECTIVENESS MULTI-ATTRIBUTE MODEL

One possible way to accomplish the 10 step cost-effectiveness evaluation on system safety is by use of system effectiveness models. In the ensuing section, system effectiveness is defined and a multi-attribute system effectiveness model is briefly explained. The reason for this overview of system effectiveness is that is is conceivably possible to use a system effectiveness model to determine and/or measure the cost-effectiveness of system safety in the development of a weapon system.

System Effectiveness deals with the capability of a system to meet its mission objectives when called upon to do so. For a weapon system, this would mean the capability to

be launched, fly the required distance, and destroy the target. In the broadest sense, it also includes the capability of the program to meet cost and schedule goals. To be effective, a system must be both ready and sustainable. [Ref. 26:p. 16-1]

Current DOD major system acquisition strategy is to build a system to meet readiness objectives, test for readiness, and if successful, field the system. If unsuccessful, modifications are to be incorporated prior to deployment.

There are many factors affecting readiness and sustainability. Major items include: reliability, availability, maintainability, (commonly called RAM); logistic responsiveness, including manpower training, support equipment, facilities, spares, and data; and funding for development, test, procurement, and operations. Of critical importance in assuring the effectiveness is the correct definition of the threat and the operating environment by the user. A system which responds to the wrong requirements cannot be cost effective.

System Effectiveness functions and responsibilities include:

- Perform reliability analyses and make reliability allocations
- Establish availability of the system
- Perform safety and hazard analysis

- Perform Failure Modes and Effects analysis and establish single point failures
- Prepare Electromagnetic Compatibility (EMC) control plan, perform Electromagnetic Interference analysis, and conduct EMC testing
- Review design for EMC compliance
- Analyze contamination sources, prepare contamination control plan, perform contamination investigations
- Prepare maintainability plan, establish maintainability timeliness
- Define acceptable parts, materials, and processes and set up control system to ensure manufacturing compliance
- Analyze designs to ensure that appropriate engineering principles have been incorporated
- Define the threat environment and establish survivability requirements.

Measures of system effectiveness, often called figures-of-merit, can provide a quantitative means of comparing alternative system configurations or comparing proposed changes with a baseline configuration. This requires integrating specialty areas into the system process to ensure a quality product.

Currently within DOD, one way to evaluate a system's effectiveness is with the aid of reliability, availability, maintainability, (RAM) and capability math models. Components of this system effectiveness model are defined in Figure 5-3.

System Effectiveness

Dependability (Reliability) (Performance)	Availability (Operate Time and Repair Time)	Capability

Reliability = probability of Systems Success for a defined mission

Availability = Probability that systems can start missions on demand

Capability = Probability of systems performing missions as required

Maintainability = The measure of the ability of an item to be retained in or restored to a specified condition when maintenance is performed by personnel having specified skill levels, using prescribed procedures and resources, at each prescribed level of maintenance.

Factors that influence reliability include:

- Design simplicity
- Parts reliability
- Environmental conditions
- Component derating
- Redundancy provisions
- Compatibility of components and parts
- Component failure rate characteristics.

Factors that influence maintainability include:

- Inherent simplicity
- Ease of accessibility
- Visibility of maintained item
- Environmental compatibility
- Safety characteristics
- Self-correcting characteristics
- Standardization
- Skill level requirements
- Self test capability
- Reduction in number of tools/special tools required.

Figure 5.3 Systems Effectiveness Composition

Availability is defined in terms of time-related factors of reliability and maintainability as follows:

- Mean-Time-Before-Failure (MTBF) is a reliability function which assumes that operation occurs after early failure (infant mortality) and prior to wear-out, i.e., a constant failure rate exists.

- Mean-Time-To-Reapir (MTTR), as a maintenance function, can include corrective maintenance time (CMT) and preventive maintenance time (PMT).

- Mean-Logistics-Down-Time (MLDT) is a maintenance-related logistics function which involves spares provisioning and includes logistic delay time (LDT) and administrative delay time (ADT).

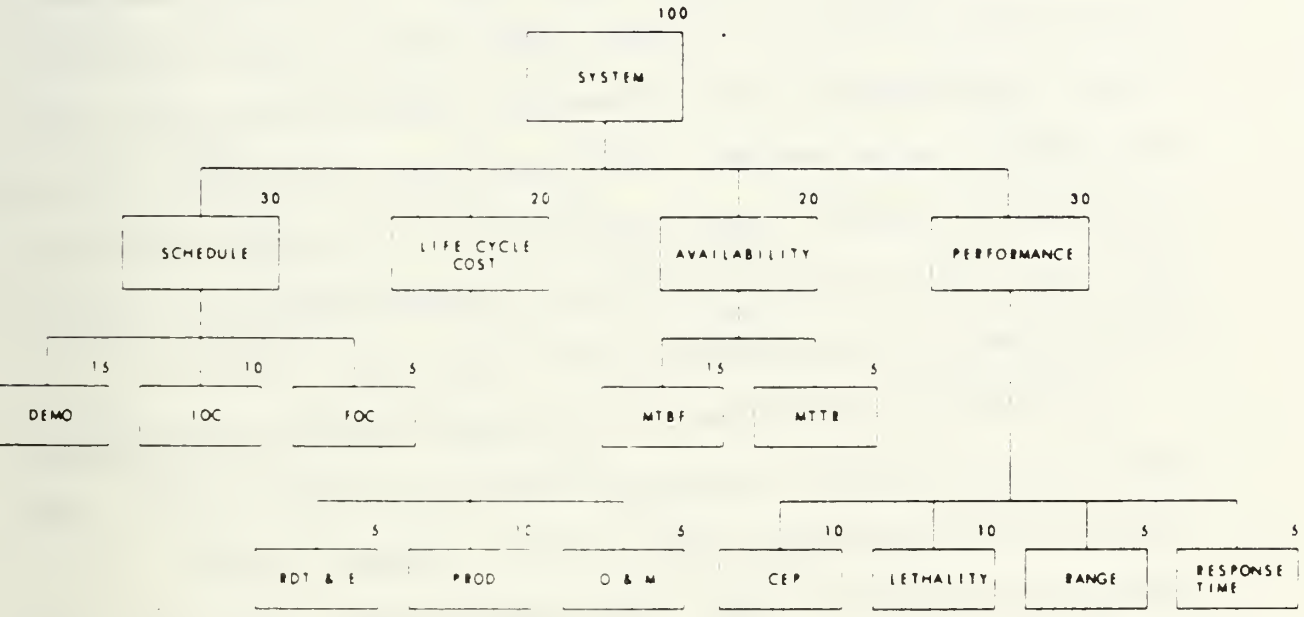
Three types of availability are commonly used with the above context--Inherent Availability (A_I), Achieved Availability (A_A), and Operational Availability (A_O).

Readiness and sustainability objectives are identified during the Concept Exploration phase, together with funding requirements. In the Demonstration/Validation phase, reliability and maintainability concepts are incorporated into the requirements and design; and support concepts, maintenance levels, sparing policy, and skill requirements are identified. In the FSD phase, readiness objectives are validated through testing, and detailed support plans are prepared. During Production and Deployment, support resources are procured and readiness objectives verified through field tests.

This effort is accomplished primarily by the engineering specialties, which are usually assigned to System Engineering from a matrix organization for a specific period.

Figure 5.3 (Continued)

System effectiveness models provide a means of evaluating alternate system configurations with respect to effectiveness categories of cost, schedule, availability, and performance. Figure 5.4 illustrates a multi-attribute model used to evaluate a system's effectiveness. Other



Source: [Ref. 26:p. 16-6]

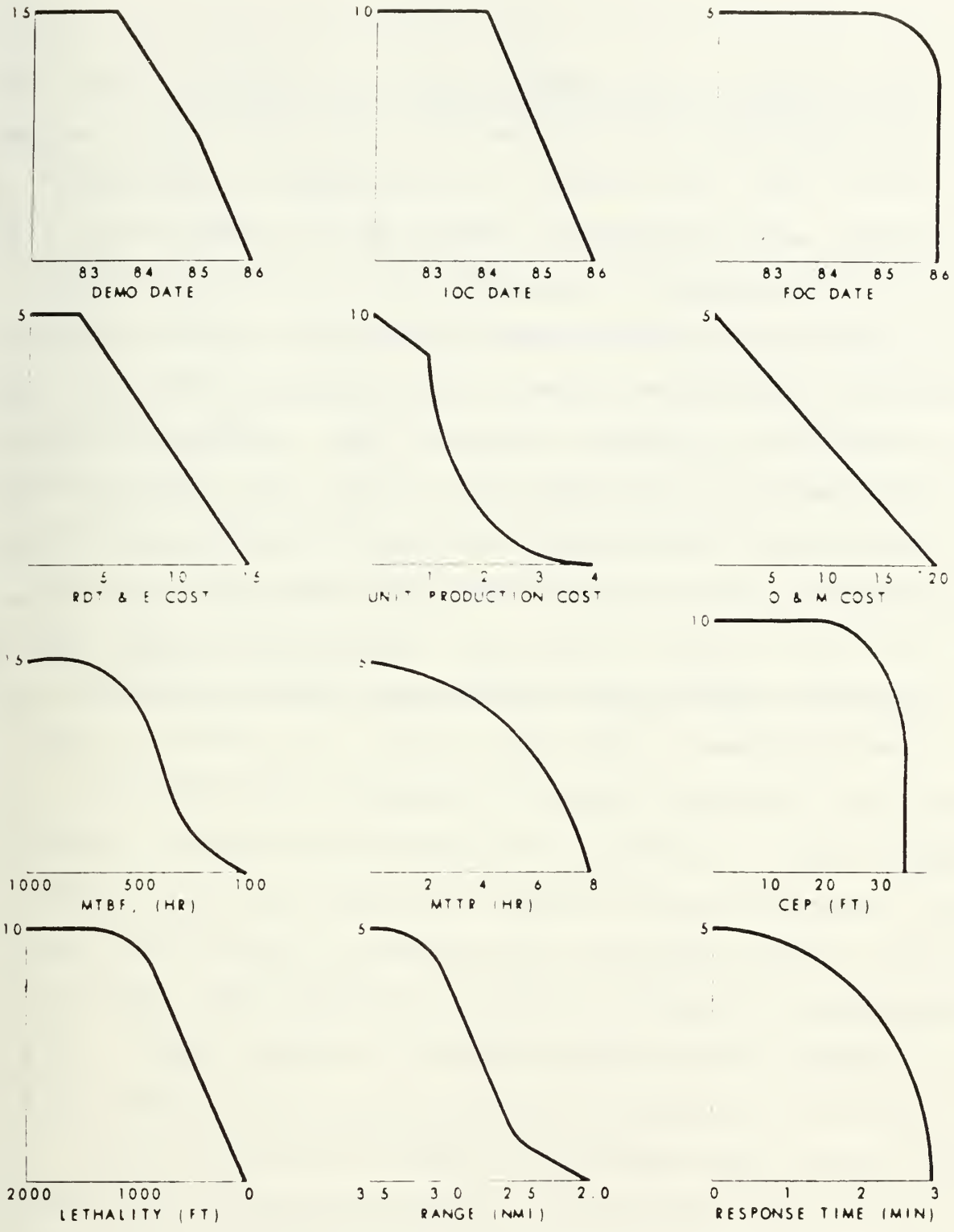
Figure 5.4 Multi-Attribute System Effectiveness Model

major categories such as standardization, "system safety," preplanned product improvement, productivity, and such could be added if these were defined as major program objectives. Lower levels of attributes provide quantitative measures which permit evaluation and ranking of candidate configurations. Each attribute is assigned a percentage of

the total system effectiveness (100) based on its relative importance of meeting mission objectives. For example, both schedule and performance are assigned the highest weights (30). At the next level down, these values are apportioned to specific measurables again according to their perceived value to overall missions objectives. In the performance area, these include: circular error probability, lethality, range and response time. These are identified as technical performance measurements. The model may be carried one or more levels further down, if desired, to provide visibility into the actual subsystem design parameters which comprise the top-level measurables. [Ref. 26p. 16-5]

Individual attributes in the model are then represented by utility function curves as shown in Figure 5.5. The utility curve represents the benefit (weight) for an achieved attribute value. Each curve covers the range from the maximum possible value (beyond which no further benefits accrue to the system), to the minimum acceptable value (below which minimum mission objectives cannot be met). [Ref. 26:p. 16-5]

The curves are established through discussions with users, operational personnel, program management, and others with knowledge of the program objectives, "often starting with a purely arbitrary curve." The shape of the curve is dependent upon the criticality of meeting the desired value and the risk that the program is willing to accept. That



Source: [Ref. 26:p. 16-7]

Figure 5.5 Utility Function Curves

is, curves that show a rapid decrease in weighing value as the attribute value departs from its maximum indicate that the performance is critical to achieving mission success and/or that the program is risk averse in this area. A linear curve represents a risk neutral position over the acceptable range of parameter values. [Ref. 26:p. 16-6]

Scoring is accomplished by specialists in each area to define the expected range of values (minimum, maximum, most likely). A distribution curve is then established from the responses for each attribute for each configuration. The weight of each attribute can then be established and the totals for each configuration scored. When the total scores are close (within 10 percent), sensitivity analyses can be conducted using maximum and minimum values to establish the least-risk case. [Ref. 26:p. 16-6]

VI. SUMMARY OF ANALYSIS/CONCLUSIONS/RECOMMENDATIONS

A. SUMMARY OF ANALYSIS

The purpose of this thesis was to determine the cost-effectiveness of system safety in the development of a weapon system. In trying to answer this research question, a one week research trip was made to the following commands: Naval Air Systems Command (NAVAIRSYSCOM), Washington, D.C.; Naval Air Engineering Center (NAEC), Lakehurst, New Jersey; and Naval Air Test Center (NATC), Patuxent River, Maryland. An overview of the findings of this trip are provided.

The organization for System Safety within the Navy is shown in Figure 6.1.

NAVAIRSYSCOM's Director of Safety (AIR-09F) provides policy guidance and management assistance. The System Safety Coordinator (AIR-516C) advises program management and field activities on technically adequate system safety programs. NAEC and NATC are field activities to NAVAIRSYS-COM. Field Activities provide system safety engineers to work system safety programs under the direction of AIR-516C.

Per the flowchart, AIR-516C is within the Systems and Engineering Department (AIR-05). Even though AIR-516C is a component of AIR-05, it hasn't received much support for fulfilling system safety requirements. AIR-516C consists of

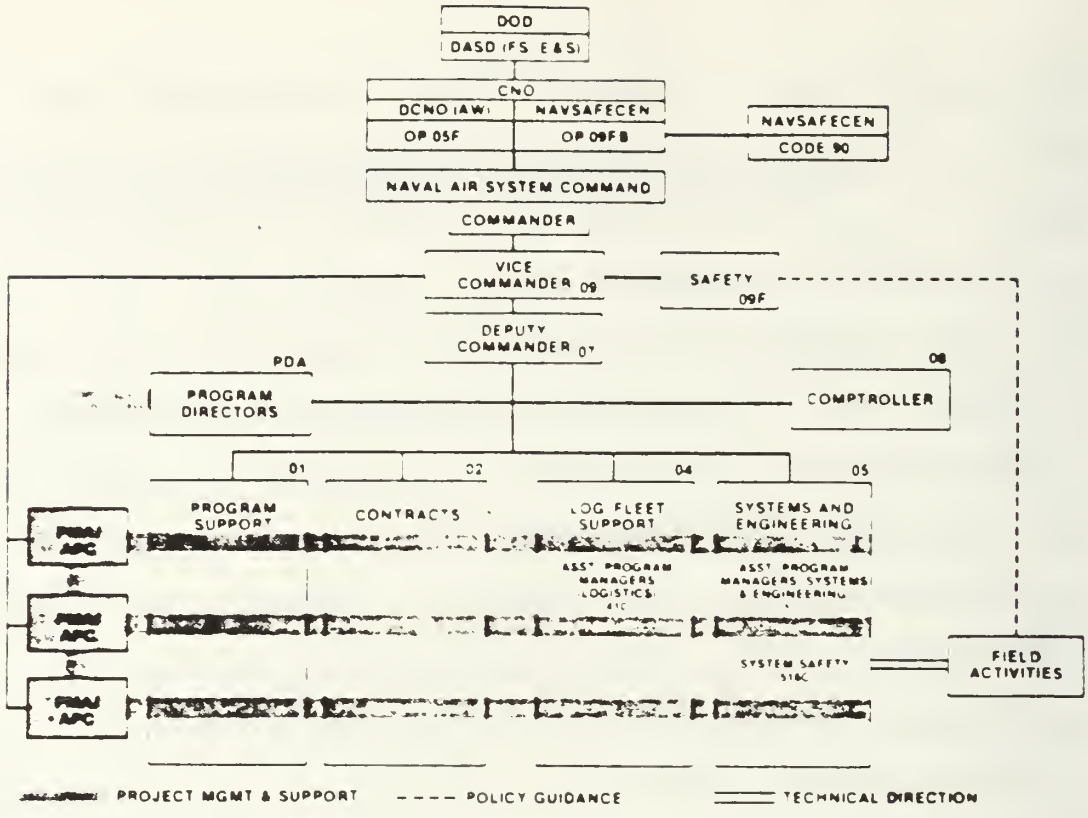


Figure 6.1 Organization for System Safety

one system safety engineer and one system safety engineering trainer. These two people are responsible for not only ensuring system safety program requirements are placed in various contractual documents but monitoring the progress of approximately 100 different aviation programs.

NAEC has a team of approximately twenty system safety engineers who assist AIR-516C via various class desk officers in managing system safety programs. A system safety manager oversees and provides guidance to these system safety engineers.

The class desk officer is the project engineering director. A class desk officer exists for each naval aircraft (i.e., F-18, CH-53, P-3) at NAVAIRSYSCOM. The class desk officer is responsible for funding NATC and NAEC system safety engineers to perform various system safety tasks. The class desk officer is also responsible for ensuring that system safety is addressed as a distinct item during all program reviews (i.e., preliminary and critical design reviews).

The NAEC team of system safety engineers was formulated to assist AIR-516C in the difficult task of monitoring high level aircraft weapon system developments. The current team of engineers are younger and have only a few years of engineering experience. Even though the team consists of younger engineers, they are dedicated to ensuring system safety requirements are fulfilled. Problems that currently exist in monitoring system safety program requirements at NAEC are as follows:

1) NAEC is a field activity to NAVAIR and yet NAEC system safety engineers work more or less directly for the class desk officer. The commanding officer of NAEC sometimes tasks the team with other requirements which hampers their ability to perform critical system safety tasks;

2) Office working conditions are below standards. Engineers are working in cramped spaces with no privacy;

3) The team is somewhat isolated from what is going on in the naval aviation community. Frequent trips must be made to NAVAIRSYSCOM which is a 4-5 hour drive from NAEC.

NATC has approximately two system safety engineers at each aircraft directorate (i.e., rotary wing, strike, and anti-submarine warfare) who also assist AIR-516C via the class desk officer. A NATC staff assistant for system safety provides technical guidance to the various NATC system safety engineers and annually audits each NATC system safety program for conformance to system safety requirements.

NATC is different from NAEC in that NATC engineers assist NAEC engineers in managing system safety programs. The reason for this is that NAEC is considered the center of excellence for aircraft system safety and as such is project principle for system safety and keeps track of all hazards identified on each aircraft program.

NATC's role then is to analyze research, development, test, and evaluation (RDT&E) system safety information and supply it to both the class desk officer and NAEC system safety project engineers. NATC engineers have somewhat of an edge over NAEC engineers because they have direct access to aircraft that are being used for (RDT&E). This direct access allows NATC engineers to have more hands-on experience in performing system safety tasks (i.e., they can directly see an aircraft that has safety design flaws or get timely information after a test flight).

Data obtained from this research trip and from various data searches and telephone conversations was not sufficient

to perform an in-depth cost-effectiveness analysis of system safety. In performing this analysis it would have been appropriate to acquire cost data and aircraft mishap statistics on various aircraft programs to compare and analyze the data. On past and current aircraft programs, system safety isn't broken out as a separate line item for costing in aircraft contracts. This made it impossible to find out what various contractors are specifically spending on system safety program requirements. A brief overview of data which was considered to be important in making some general assumptions regarding the cost-effectiveness of system safety will be reviewed.

The all-Navy mishap rate[1] is presented in Figure 6.2. This figure points out various safety programs that have been implemented since 1954. As depicted in the graph, the Navy mishap rate has been declining. Two views presently exist on maintaining and/or further decreasing the Navy's already low mishap rate. They are: 1) train Navy pilots to be more safety conscious, or 2) better technology. Each of these views make sense but why isn't System Safety considered a viable alternative? Most likely it is because

---

[1]Mishape rate--mishap rates are generically determined as follows:

$$\frac{\text{Total flight hours for all-navy aircraft for one year}}{100{,}000} = X$$

$$\frac{\text{Total Class A mishaps for that same year}}{X} = \text{Mishap rate for Class A mishaps}$$

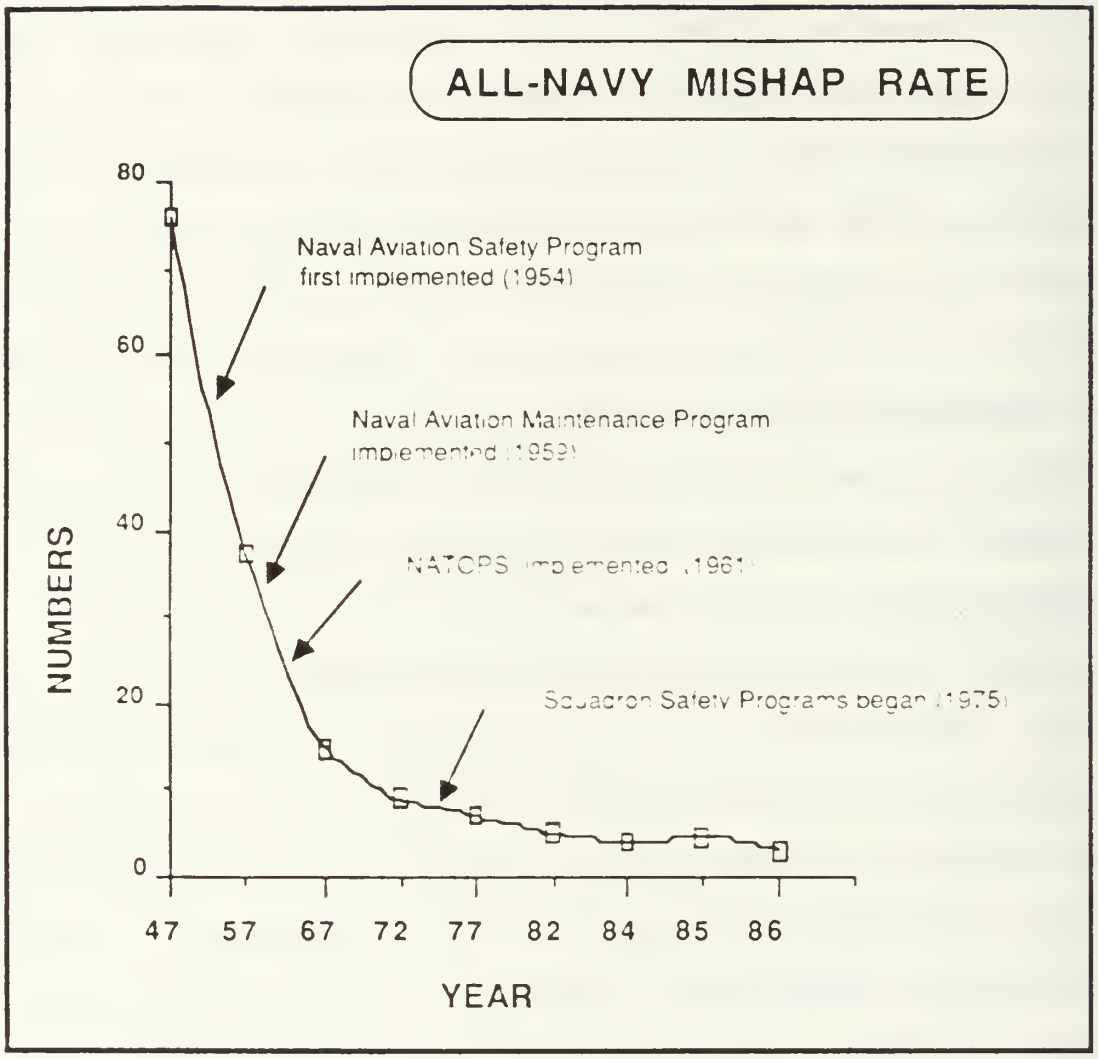


Figure 6.2 All-Navy Mishap Rate

not everyone is aware of the system safety concept and what it can do in preventing aircraft mishaps. The inability of system safety to be quantifiably measured in obtaining

operational effectiveness requirements is considered a contributing factor.

Figure 6.3 shows costs of Class A mishaps in 1986 dollars. Fiscal year 1986 wasn't a good year for aircraft mishap costs. In 1986 aircraft mishap costs were $221 million. $221 million only represents aircraft costs. It does not include costs due to injury or death. Even though the Navy may be having fewer mishaps, the aircraft that were damaged or destroyed in 1986 due to mishaps cost more.

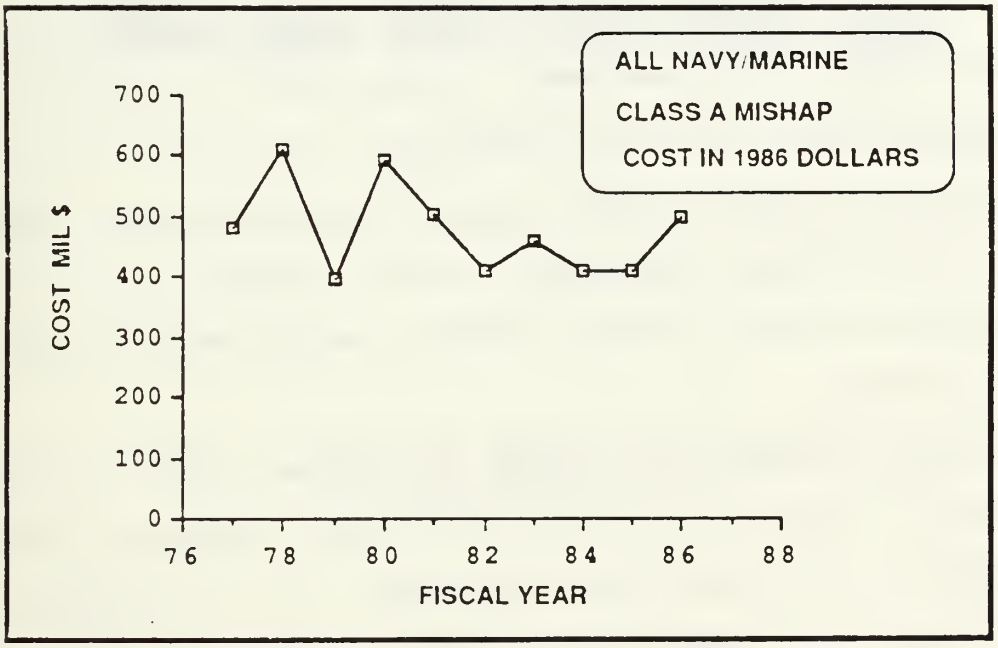


Figure 6.3 All Navy/Marine Class A Mishap Cost in 1986 Dollars

This is what each type of navy aircraft costs in thousands of dollars:

Aircraft	Column A	Column B
F/A-18	$22,800	$33,880
F-14 A/B	#17,826	$44,544
EA-6B	$19,200	$39,942
AV-8B	$18,000	$21,283
A-6E	$12,200	$35,700
P-3C	$14,800	$54,060
E-2C	$25,200	$59,950
C-2A	$13,400	$21,263

Column A is per the Naval Safety Center and represents what each aircraft cost when originally acquired. The Naval Safety Center data was used in Figure 6.3. Column B is per Aviation Week and Space Technology and represents current replacement costs. There is quite a difference. Aviation Week and Space Technology cost figures are a truer indication of what a Naval aircraft would cost to replace in 1986 dollars.

Major reasons for Class A mishpas are as follows. Figure 6.4 shows All Navy/Marine Class A mishaps by phase of operations. As shown, most accidents occur in flight.

Figure 6.5 shows causal factors for Class A mishaps. Most mishaps are due to pilot error but material failure is next in line. Causal factors for pilot error are as follows:

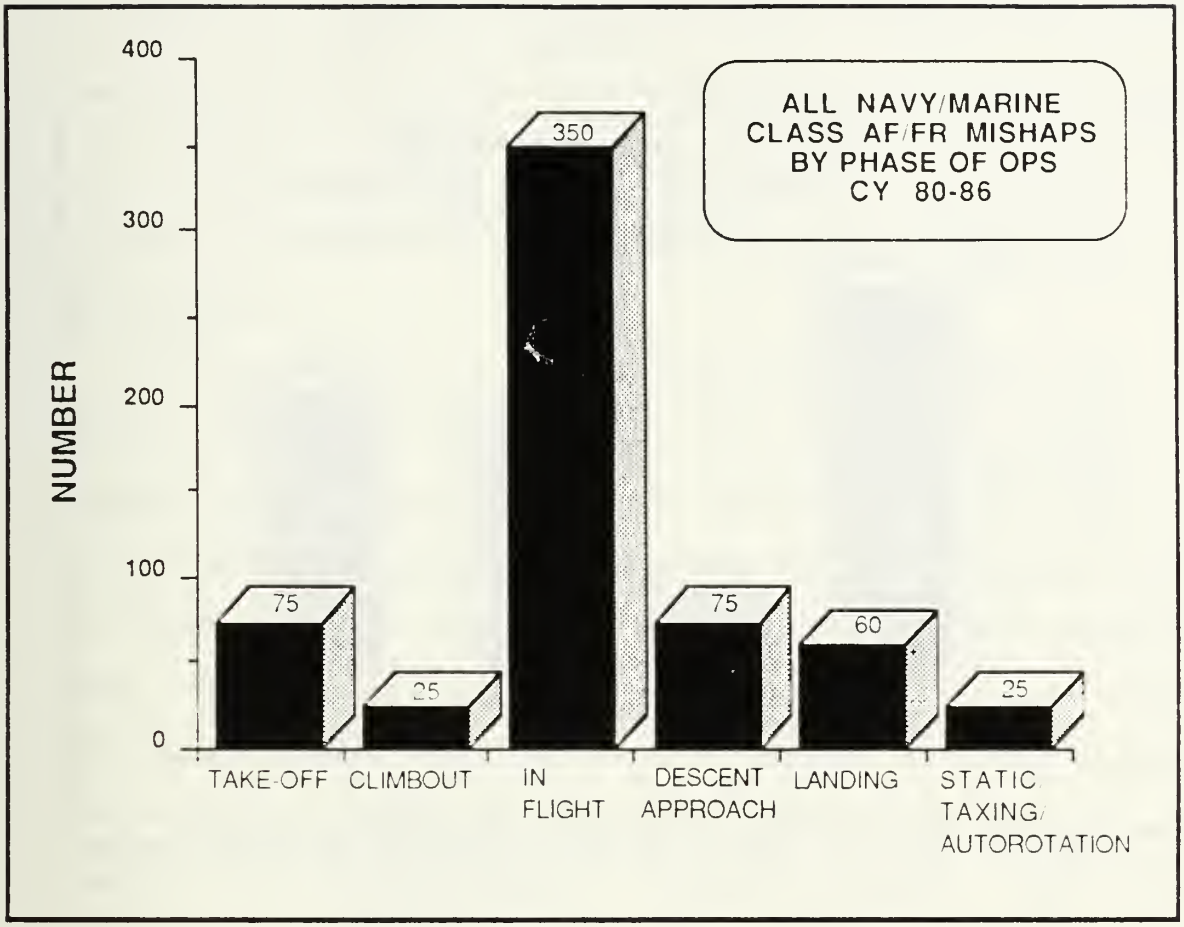


Figure 6.4 All Navy/Marine Class A Flight & Flight Related Mishaps by Phase of OPS, CY 80-86

1. Misuse of flight controls
2. Violation of regulations/flight manual
3. Physical/mental condition
4. Inadequate flight preparation
5. Faulty performance by other pilot in aircraft

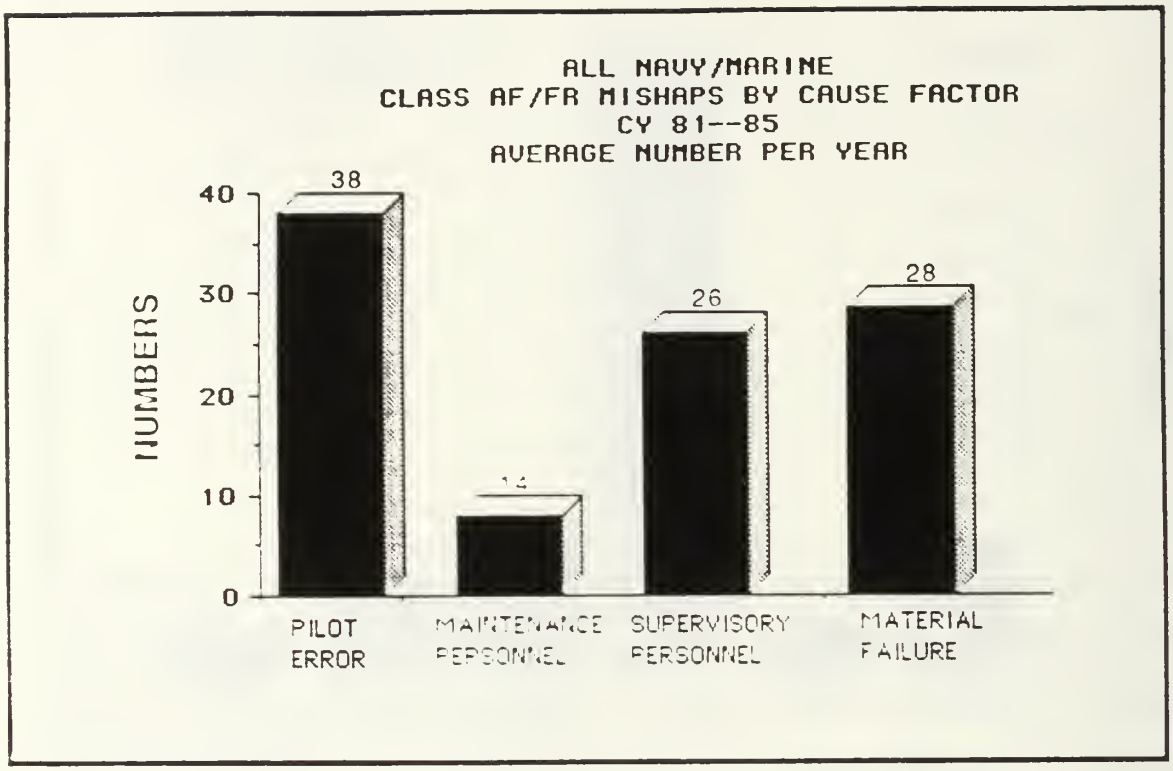


Figure 6.5 All Navy/Marine Class A Flight & Flight Related Mishaps by Cause Factor, CY 81-85, Average Number per year

6. Failure to maintain flying speed

7. Failure to recognize a dangerous situation

8. General errors in judgment

9. Misjudgment of distance/altitude/position.

Mr. Jim Gibble, NAVAIRSYSCOM's Director of Safety (AIR-09F), states that:

system safety can improve not on material failure mishap causal factors but pilot error mishap causal factors by having human factors and design engineers to not only consult with system safety engineers but to have them

ensure that system safety hazards are either eliminated or controlled to an acceptable level during an aircraft weapon system's development.

Figure 6.6 shows safety improvement in navy fighter aircraft mishaps during the first 100,000 flight hours. The F/A-18 exhibits a far better accident rate than its predecessors.

The F-14A had a modest system safety program. No navy system safety expertise was available. Although the initial mishap rate was significantly lower than expected, inflight fires and engine problems resulted in a significant number of mishaps. The Logistics Management Institute estimates that the engineering change costs to correct safety deficiencies over the life of a program is $110 million. One causative agent for inflight fires on the F-14A was the design of a radar liquid cooling system. The fires originated when the cooling fluid sprayed from a failed elapsed time indicator onto hot surfaces or electrical equipment which caused ignition. Before the problem was identified and corrected, $12.8 million was lost in mishaps and was a suspected causal factor in two other unexplained F-14A losses. If the potential for a coolant leak had been anticipated, corrective action could have been taken during the development cycle. With increased emphasis on system safety this type of problem can be identified during the development cycle and eliminated.

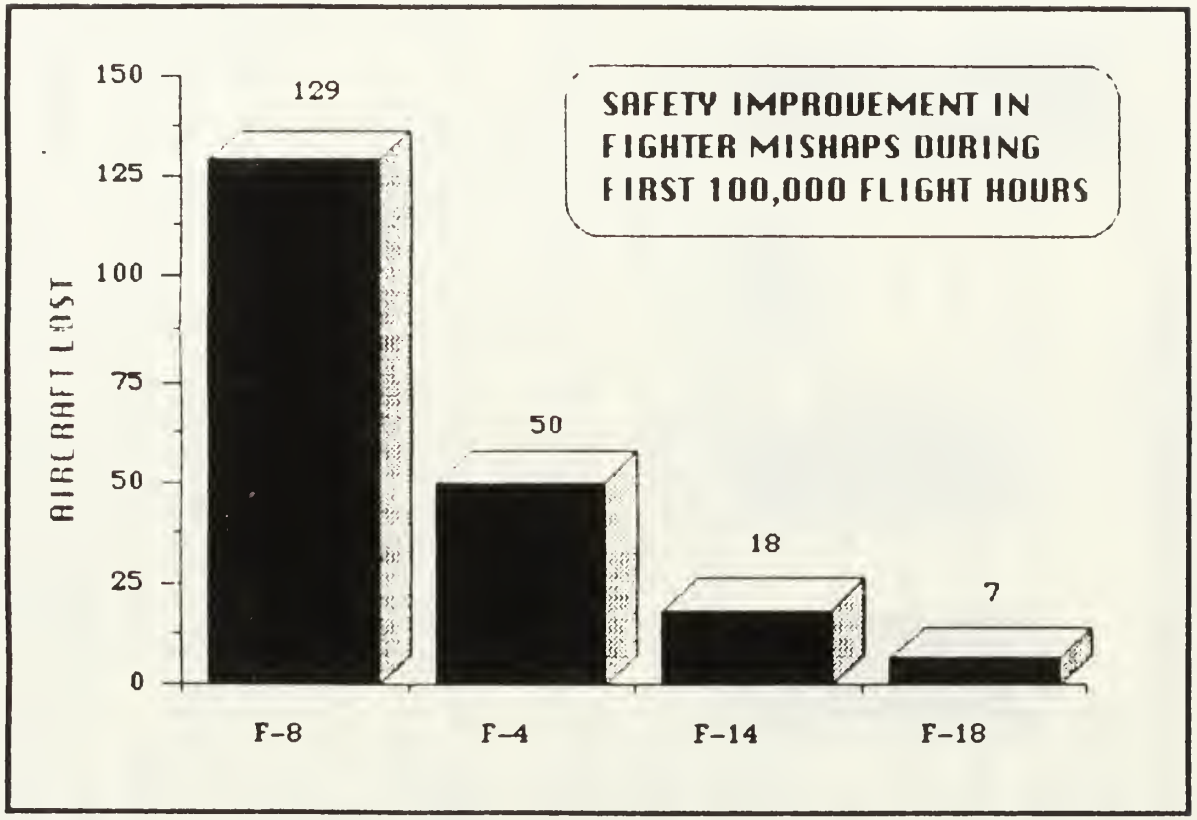


Figure 6.6 Safety Improvement in Fighter Mishaps During First 100,000 Flight Hours

In summary, the F-18 had a more extensive system safety program and is a good example of what an aggressive system safety effort can contribute to the Navy. The cumulative F/A-18 class A mishap rate is 7.07 per 100,000 flight hours. The F-14A Class A rate at equivalent flight hours was 18.42. If the F-18 system safety effort prevented the loss of only one F/A-18, that would save the Navy $22.8 million. Currently, the benefit/cost ratio of system safety is thought to be betwee 4 to 1. Without further analysis, it is impossible to determine an exact ratio. What is apparent is that system safety can pay for itself in the development of a weapon system if it only saves the loss of one expensive aircraft.

B. CONCLUSIONS

In conclusion of my analysis of the cost-effectiveness of system safety, system safety has received federal regulatory approval per DODINST 5000.36, "System Safety Engineering and Management." Executive Order 12291 was previously discussed somewhat in-depth. Per Executive Order 12291, regulatory action shall not be undertaken unless the potential benefits to society from the regulation outweigh the potential costs to society. In this regard, system safety should be viewed as having benefits that outweigh its costs to society.

Naval Air Systems Command directs that system safety shall be required in the development of all ACAT I and II

aircraft programs. This requirement hasn't received the emphasis that maybe it should be receiving. It was discussed that system safety is considered an engineering specialty in the system engineering process. In the real world system safety doesn't seem to play a major role in either determining technical performance measurements or in obtaining system effectiveness objectives. Yet, system engineering specialties are required to ensure system operability.

The system effectiveness model which was described is a possible way of determining the cost-effectiveness of system safety. Even though system safety isn't a component of the model, it is felt that system safety has positive effects in obtaining system effectiveness objectives.

The reason system safety isn't used as a determining factor in the effectiveness of a system may have to do with the fact that it is not perceived as an integral requirement in meeting the program objectives of cost, schedule, and performance though it should be.

System safety really encompasses the overall program by identifying hazards and minimizing risks through the entire life cycle of a system. System safety focuses not only on the total system but virtually every component of the system. Ideally a system and its components should function safely forever. In the real world this is impossible (i.e. an airplane engine is going to quit running now and then or

a control system may infrequently fail to operate). Therefore, the goal of system safety is to reduce such malfunctions as much as possible.

Although project managers and design and engineering forces usually have safety considerations on their mind as they go about designing manufacturing, producing, and maintaining a system, it is really important to assign a team of safety engineers to be a part of this process. The system safety team scrutinizes various components and, utilizing historical and empirical data, mishap reports, and their own engineering knowledge and experience, system safety engineers not only examine components on an individual basis, but take measures to ensure that components function properly when combined with others. They are concerned with the "total package" as well as the separate parts. Their attention to the "total" system in essence enhances the quality of the system and contributes not only to the performance of the system but to the reduction of future costs by having not only fewer aircraft mishaps but by producing a more reliable, maintainable, and safer system.

C. RECOMMENDATION

This thesis did not answer the primary and subsidiary research questions as it was intended to do. An inability to get adequate data was the major contributor. In summary, it is strongly recommended that the information which has

which has been provided in this thesis be used in a follow-on thesis so that a more in-depth analysis of the cost-effectiveness of system safety can be accomplished.

APPENDIX

NASA CONTRACTOR REPORT 3534--A SYSTEM SAFETY MODEL FOR DEPARTMENTAL AIRCRAFT

EXECUTIVE SUMMARY

This document presents some basic tenets of safety as applied to developmental aircraft programs. It does not discuss the philosophy of system safety nor does it present instructions for applying system safety principles to a project. Rather, the integration of safety into the project management aspects of planning, organizing, directing, and controlling is illustrated by examples. The examples presented here are taken from the joint NASA/Army Rotor System Research Aircraft (RSRA) project which has maintained an enviable safety record through several years of development and operation.

The RSRA project was initiated in 1973 to produce vehicles for conducting advanced rotor systems research. The project resulted in production of two highly instrumented aircraft capable of flying in the fixed-wing, helicopter or compound modes. The specifications established a performance envelope that exceeded normal helicopter performance in many ways while stressing adaptability to new rotor systems, precisely controlled test conditions, and measurement accuracy. Fulfillment of these specifications required advancement of state-of-the-art technology in many areas, such as provision for crew escape in an emergency. It also required close coordination between NASA and contractor personnel. This, in turn, necessitated formulation of unusual communication protocols which fostered development of a "project family" attitude.

The RSRA project office was originally based at Langley Research Center and operated within confines of a typically austere research and development budget. During later stages of development the project was transferred to the Ames Research Center resulting in general loss of corporate memory and necessitating changes in the system safety program to compensate for this loss.

To begin an overview of the RSRA safety program, it would be well to understand the attitude and philosophy of the former RSRA Project Manager/Chief Engineer, Sam White,

Jr. His approach to safety on the project was guided by the following philosophy:

The system safety program that evolved on the RSRA was based on a set of concepts, some basic system safety principles, and on a fairly limited set of guidance documents. A list of some pretty basic (yet very useful) principles was used in developing the RSRA system safety program (courtesy of Chuck Miller's George Washington University program on aviation safety):

a. Accidents are unplanned, but controllable combinations of events.

b. Accidents are rare; hazards (risks) are not.

c. Combinations of "acceptable" hazards produce accidents.

d. Accidents are usually caused by a sequence of complex cause-effect relationships that may be obscured by simplistic probable/proximate cause determinations.

e. Cause-prevention determination should include factors of:

- Man (human error, workload)
- Machine (failure, design defect)
- Medium (environment)
- Management (attitude, motivation, control)
- Mission (nature, urgency)
- Money (cost/safety tradeoffs).

f. Safety is an integral part of mission accomplishment (economic, survival).

g. Accident prevention is more than accident investigation and cause-corrective action determination.

h. Managers/supervisors can delegate/assign safety authority/actions but cannot delegate accountability.

i. A data bank of known precedents exists for risks and corrective actions.

j. Hazard/accident reporting must emphasize corrective action, including rule enforcement, without seeking to punish improper action.

k. Human hyperawareness of high risk often results in a higher level of safety.

l. Safety tasks are finite, identifiable, definable, and do-able. Competently done, they reduce accidents.

- Define requirements (process and results, not procedures: What, not how)
- Prepare plans (road map, who/what/when)
- Conduct hazard analyses
- Develop emergency as well as normal procedures
- Conduct program reviews (use jury approach)
- Influence behavior (educate, train, indoctrinate, motivate, correct)
- Conduct surveys, audits, inspections
- Use known precedent centers
- Investigate accidents/incidents (determine cause, take corrective action, follow-up)
- Provide staff "Chaplain," ombudsman (opens free communication, emphasizes correction, deemphasizes punishment, provides liaison).

The list of safety tasks under the last bullet is particularly useful in planning a system safety program.

The applications of these and the other basic principles are illustrated in detail throughout the text.

The methods by which safety would be achieved were documented in an Air-worthiness Qualification Plan (AQP) developed early in the project. The requirements specified by the AQP were carefully tailored to fit the specific RSRA mission objectives and to satisfy the intent of agency criteria.

The RSRA project budget did not permit a large safety cadre. Therefore, a safety focal point was established and the entire project staff became involved in the attainment of safety objectives. Safety goals became project goals and increased safety consciousness of the staff resulted. Resource allocations were altered when necessary to provide for performance of safety tasks of most benefit. This "horse-trading" of resources involved some risk which project management accepted when necessary, but as a conscious act, not through ignorance or default. This bold stance was justified because management remained deeply involved in safety activities throughout project development.

In the final synopsis of RSRA safety experience, it should be noted that safety goals were given in terms of

positive actions. That is, negative connotations were avoided with reference to safety, and attitudes were fostered to keep safety in concert with other project activities.

It was recognized early in the project that even ultra-attention to safety in the design and ground test phases would not assure operational safety without in-depth knowledge and awareness by the flight team. For this reason, both Government and contractor flight crews were involved throughout the design, development, test and evaluation (DDT&E) process.

While the RSRA experience was not a perfect example of "doing everything right," it came close. Some painful lessons were learned, especially relative to safety impacts of schedule slippages, transfers of roles and missions, and associated loss of corporate memory. However, flexibility was found to be a key. When events beyond project management control led to schedule impacts, slippage was allowed, but not loss of project control.

In the words of the RSRA Chief Engineer,

> The fact that the project matured effectively and without incident is believed to be a direct result of the breadth and depth of safety planning and the in-depth involvement of all hands in safety plan implementation. The point is that the energies devoted to safety tasks are not all penalties to be suffered out of the need for safety; they produce benefits that enhance operational efficiencies, safety aside.

LIST OF REFERENCES

1. Covault, Craig, "Rogers Commission Charges NASA with Ineffective Safety Program," Aviation Week and Space Technology, Vol. 124, pp. 18-22, June 16, 1986.

2. Logistics Management Institute, System Safety in Aircraft Acquisition, by F. Ronald Frola and C.O. Miller, January 1984.

3. Naval Safety Center Unclassified Letter: unserialed to Chief of Naval Operations (OP-09BF), Subject: Navy System Safety Program Objective Memorandum (POM) 89 Funding Request, 26 November 1986.

4. U.S. Army Agency for Aviation Safety, Preparation of a System Safety Program Plan for Aviation Systems Development (final report). USAAAVS-TR-72-8, AD-741-364.

5. Olson, Richard E., System Safety Handbook for the Acquisition Manager, Prepared by Aerospace Corpration for Space Division, Air Force Systems Command, Document Number 5D-GB-10, 10 December 1982.

6. Roland, Harold E. and Brian Moriaty, System Safety Engineering and Management. John Wiley & Sons, 1983.

7. Department of Defense Military Standard MIL-STD-882B, System Safety Program Requirements, 30 March 1984.

8. Layton, Donald M., DOD System Safety Management and Engineering. Naval Postgraduate School, 1986.

9. Amberboy, Emil J. and Robert L. Stokeld, A System Safety Model for Developmental Aircraft Programs, NASA-CR-3534, April 1972.

10. Hammer, Willie, Handbook of System and Product Safety. Prentice-hall, Inc., 1972.

11. Sassione, Peter G. and William A. Schaffer, Cost-Benefit Analysis: A Handbook. Academic Press, Inc., 1978.

12. Smith, Kerry, "A Conceptual Overview of the Foundations of Benefit-Cost Analysis," pp. 13-34, In: Benefits Assessment: The State of the Art, Judith D. Bentkover et al. (Eds.), D. Reidel Publishing Company, 1986.

13. Layard, Richard, Ed., Cost-Benefit Analysis, 3rd Ed., Richard Clay (The Chaucer Press), Ltd., 1976.

14. Gramlich, Edward M., "Benefit-Cost Analysis of Government Programs," In: Benefit, Cost, and Beyond, by James T. Campen, Ballinger Publishing Co., 1986.

15. Campen, James T., Benefit, Cost, and Beyond, Ballinger Publishing Company, 1986.

16. Sugden, Robert, and Alan Williams, "Principles of Practical Cost-Benefit Analysis," In: Benefit, Cost, and Beyond, by James T. Campen, Ballinger Publishing Co., 1986.

17. Stokey, Edith, and Richard Zechauser, "A Primary for Policy Analysis," In: Benefit, Cost, and Beyond, by James T. Campen, Ballinger Publishing Co., 1986.

18. Musgrave, Richard A. and Peggy B. Musgrave, "Public Finance in Theory and Practice," In: Benefit, Cost, and Beyond by James T. Campen, Ballinger Publishing Co., 1986.

19. Mishan, E.J., "Cost-Benefit Analysis," In: Benefit, Cost, and Beyond by James T. Campen, Ballinger Publishing Co., 1986.

20. Pearce, D.W., "Cost-Benefit Analysis" In: Benefit, Cost, and Beyond, by James T. Campen, Ballinger Publishing Co., 1986.

21. Hitch, C.J., "Decision Making for Defense," In: Cost-Effectiveness: The Economic Evaluation of Engineering Systems by John ENglish Morley, John Wiley & Sons, Inc., 1968.

22. English, John Morley, Ed., Cost-Effectiveness: The Economic Evaluation of Engineering Systems, John Wiley & Sons, Inc., 1968.

23. Quade, Edward S., "Introduction and Overivew," In: Cost-Effectiveness Analysis: New Approaches in Decision-Making by Thomas A. Goldman, Frederick A. Praeger, Inc., 1967.

24. Bentkover, Judith D. et al. (Eds.), Benefits Assessment: The State of the Art, D. Reidel Publishing Co,, 1986.

25. Little, Arthur D., Cost-Effectiveness in Traffic Safety, Frederick A. Praeger, Inc., 1968.

26. Defense Systems Management College, System Engineering Management Guide, Fort Belvoir, Virginia, October 1983.

27. Kazanowski, A.D. et al., "A Standardized Approach to Cost-Effectiveness Evaluations," In: Cost-Effectiveness: The Economic Evaluation of Engineering Systems by John Morely (Ed.), John Wiley & Sons, 1968.

INITIAL DISTRIBUTION LIST

		No. Copies
1.	Defense Technical Information Center Cameron Station Alexandria, Virginia 22304-6145	2
2.	Library, Code 0142 Naval Postgraduate School Monterey, California 93943-5002	2
3.	Naval Safety Center Attn: Paul Kinzey Naval Air Station Norfolk, Virginia 23511-5796	1
4.	System Safety Engineering Attn: Richard E. Olson Department of the Air Force Headquarters Space Division--SE P.O. Box 92960, Worldway Postal Center Los Angeles, California 9009-2960	1
5.	Prof. Donald M. Layton, Code 67Ln Naval Postgraduate School Monterey, California 93943-5000	1
6.	Prof. Paul M. Carrick, Code 44Ca Naval Postgraduate School Monterey, California 93943-5000	1
7.	LCDR Dale Scoggin, Code 54Sc Naval Postgraduate School Monterey, California 93943-5000	1
8.	Commander Naval Air Systems Command (AIR-09F) Naval Air Systems Command Headquarters Washington, D.C. 20361-0001	3
9.	Commander Naval Air Systems Command (AIR-516C) Naval Air Systems Command Headquarters Washington, D.C. 20361-0001	1
10.	Prof. David R. Whipple, Code 54Wp Naval Postgraduate School Monterey, California 93943-5000	1

11. Naval Air Test Center — 1
    Attn: Jack Copeland
    System Safety Department
    Patuxent River, Maryland, 20670-5304

12. Commanding Officer — 2
    System Safety Engineering Department
    Attn: Dave Marcinick
    Naval Air Engineering Center
    Lakehurst, New Jersey 08733-5000

13. Lt Alberta Rose Jones — 3
    154 Royal Court
    Vallejo, California 94591

14. LT Barry Graham — 1
    HQ ASD/AFS
    Wright Patterson Air Force Base, Ohio
    45433-6503

Thesis
J6755 Jones
c.1 Cost-effectiveness
analysis of system safety.